DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL SEDE MERCEDES PARDO DE SIMMONDS DE LA CIUDAD DE POPAYÁN.

JENNY FERNANDA RESTREPO SANTACRUZ

UNIVERSIDAD ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

POPAYAN- CAUCA

2017

DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL SEDE MERCEDES PARDO DE SIMMONDS DE LA CIUDAD DE POPAYÁN.

JENNY FERNANDA RESTREPO SANTACRUZ

TRABAJO DE GRADO COMO REQUISITO PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. JULIO ALBERTO VARGAS
Asesor de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

POPAYÁN- CAUCA

2017

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha de entrega

DEDICATORIA

A Dios que es mi guía en cada proyecto emprendido, a mi hijo Juan Sebastián, a mis padres y hermanos, por su incondicional apoyo, comprensión y motivación, son ustedes el pilar de mi vida, el motor que me impulsa a ser mejor cada día.

AGRADECIMIENTOS

Gracias a Dios por bendecirme y guiarme en el transcurso de este bello camino, a mi hijo por su comprensión, a mis padres y hermanos por ser mi fortaleza en los buenos y en los malos momentos, a los tutores que han hecho parte de esta formación, por su dedicación y valiosas enseñanzas.

CONTENIDO

pág.

LISTADO DE TABLAS

pág.

LISTADO DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

1. INTRODUCCIÓN

Debido al crecimiento avanzado de las tecnologías de la información en la actualidad podemos indicar que estas son la base fundamental en la realización de actividades en los diferentes entornos como la salud, la educación, el comercio, el transporte entre otros, pero debido a ello también ha dado lugar a diversos conflictos ya que está expuesto a múltiples ataques que ponen en riesgo la seguridad de la información de las organizaciones.

Teniendo en cuenta que uno de los activos más importantes que posee una organización es la información, estas necesitan proteger dicho activo basado en las normas de las entidades certificadas, que brindan una guía para el diseño de un sistema de gestión de la seguridad de la información, que está fundamentada en una política creada de acuerdo a las necesidades de una organización, una de esas normas que serán aplicadas con dicho fin es la ISO/IEC 27001: 2013 para la realización del diagnóstico del estado actual de la seguridad información en el proceso de gestión académica de la Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds que es una empresa pública del sector de la educación.

2. PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción del problema

La Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, es una institución que ofrece sus servicios educativos a 520 estudiantes, sus instalaciones físicas cuentan con los requerimientos necesarios para la educación de los niños, además cuenta con equipos tecnológicos de última generación tales como una sala de tecnología e informática dotada de 40 computadores portátiles, 10 computadores de mesa video beam, micrófono inalámbrico, cabina activa, sala de audiovisuales, la institución cuenta con un servicio de internet de 20 Gb.

A pesar de que la institución educativa cuenta con las herramientas tecnológicas adecuadas para optimizar su progreso a nivel educativo y administrativo, este no cuenta con un sistema que garantice la seguridad de la información, motivo por el cual está en riesgo eminente debido a la cantidad de información que se maneja en el proceso de gestión académica; como el ingreso de calificaciones, creación de logros e indicadores de logro, por periodos académicos establecidos por la institución, generación de informes de calificaciones de cada estudiante información que es creada y modificada por medio de una aplicación web, la cual no cuenta con las políticas de seguridad adecuadas, aunque cuenta con contraseñas de usuario estas no están cifradas, los certificados emitidos por la institución no cuentan con la seguridad necesaria de un documento digital.

Lo que se busca en la Institución es realizar en primera instancia un diagnostico al estado actual de la seguridad informática basada en el estándar ISO 27001:2013 que permita identificar las vulnerabilidades, amenazas y riesgos a los que está expuesta la institución educativa en el proceso de gestión académica .

2.2. FORMULACIÓN DEL PROBLEMA

¿Cómo es posible recomendar a la Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, medidas de seguridad para protegerse y mantener la confidencialidad, integridad y disponibilidad de la información?

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar un diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013 que le brinde a la institución educativa el contexto de cómo está tratando la seguridad de la información y las mejoras que se pueden implementar en su proceso.

3.2. OBJETIVOS ESPECÍFICOS

Identificar los procedimientos actuales de la institución educativa Técnico Industrial sede Mercedes Pardo de Simmonds para la ejecución de sus actividades en el proceso de gestión académica.

Identificar y valorar los activos de información disponible en la Institución Educativa Técnico Industrial sede Mercedes Pardo de Simmonds.

Identificar los posibles riesgos de los activos de información, sus vulnerabilidades y amenazas, así como su probabilidad de ocurrencia y el impacto de los mismos.

Realizar un análisis al aplicativo web de calificaciones orientado a identificar las vulnerabilidades que ponen en riesgo la seguridad de la información de la Institución Educativa Técnico Industrial sede Mercedes Pardo de Simmonds.

Presentar el diagnóstico del estado actual de la seguridad de la información de la Institución Educativa Técnico Industrial sede Mercedes Pardo de Simmonds con sus respectivas recomendaciones de mejora y de implementación basado en la norma ISO 27001:2013.

4. JUSTIFICACIÓN

A través del diagnóstico de la seguridad de la información basada en la norma ISO 27001; 2013 que se realizará a la Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, se podrá identificar el impacto y la probabilidad de ocurrencia de vulnerabilidades, amenazas y riesgos a los que está expuesta la institución en relación a la seguridad información en el proceso de gestión académica , en el cumplimiento de sus principales pilares de la seguridad como lo es la confidencialidad, integridad y disponibilidad y como está directamente relacionado con el cumplimiento de los objetivos estratégicos de la institución y su misión.

Se realizará un análisis minucioso en donde se podrá identificar los procedimientos con mayor amenaza y su nivel de riesgo en cada uno de sus elementos que presenta la institución y que requieren un control oportuno dentro del proceso de gestión académica, y que la institución pueda plantear una acción inmediata para eliminar o minimizar dicho riesgo de acuerdo a los estándares establecidos para dicho análisis.

Es de vital importancia para cualquier organización o empresa identificar los riesgos y los impactos causados en la seguridad de la información ya que este es considerado uno de los activos más importantes, para poder así realizar una mejora continua en la gestión de la seguridad de la información basado en los resultados arrojados en un diagnóstico que permitan reducción de los diversos riesgos a los que está expuesto como la perdida de información, falta de disponibilidad, robo de información, espionaje, virus informáticos , entre otros y que permitan la continuidad y el buen funcionamiento en las diferentes áreas y procesos realizados por la institución. Adicional a ello también le permite a reducir los costos y el tiempo asociado a los incidentes y la gestión de los riegos, también mejora la implicación y participación de cada uno de los empleados de las diferentes dependencias en la gestión de la seguridad, lo que permite reforzar la confianza y la imagen de la institución, estos controles se realizaran siguiendo la norma ISO 27001-2013, en donde se le sugiere a la institución la implementación de los controles requeridos de acuerdo a los hallazgos arrojados en el análisis realizado , estos controles contribuyen a la seguridad de la información de la Institución en todos sus niveles protegiendo de forma asertiva sus activos de información, de igual manera genera un sentido de pertenencia en cuanto a seguridad en cada uno de sus empleados para la planeación, identificación e implementación de controles que puedan proteger la información .

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

En el presente proyecto se busca diagnosticar la seguridad de la información basada en la norma ISO 2700: 2013 a la Institución Educativa, con el fin de determinar y disminuir el impacto y la probabilidad de ocurrencia de amenazas, vulnerabilidades y riesgos a los que está expuesta en el proceso de gestión académica.

Para el desarrollo del diagnóstico se realizará la recolección de información de las áreas adyacentes al proceso gestión académica, con el fin de identificar los activos de información que hacen parte del proceso y detectar las amenazas, vulnerabilidades y riesgos por medio de una revisión basada en el estándar ISO 27001:2013, con dicha recolección de información y posterior detección de riesgos se procederá a establecer los controles necesarios de acuerdo a la declaración de aplicabilidad extraída en el anexo A ISO 27001 ,una vez identificados los controles que no se están cumpliendo se procederá a dar la respectivas recomendaciones para lograr el cumplimiento de los mismos.

6. MARCO REFERENCIAL

6.1. Antecedentes

Con el fin de investigar los avances obtenidos en la seguridad informática y de la información basada en el estándar ISO 27001 se consultó en diferentes proyectos que nos permiten visualizar y contextualizar la seguridad , el estándar y la forma de aplicarlo por medio de las auditorias, de acuerdo a los resultados obtenidos en los siguientes proyectos

- En el 2013 se presentó a la universidad Autónoma de Occidente de Santiago de Cali el trabajo de grado del programa de Ingeniería informática “IMPLEMENTACIÓN DE LOS CONTROLES ASIGNADOS AL DOMINIO “GESTIÓN DE ACTIVOS”, BAJO LOS LINEAMIENTOS ESTABLECIDOS POR LA NORMA ISO/27001 ANEXO A, PARA LAS EMPRESAS MUNICIPALES DE CALI, EMCALI E.I.C.E-ESP”, presentado por PAUL ROSEMBERG ENRIQUEZ ESPINOSA.

Este trabajo nos permite conocer los lineamientos de la ISO 27001 y la forma en la que se aplica el sistema de gestión de la seguridad de la información identificando los activos fundamentales de una organización y los controles que estos deben tener y que permita la reducción de los riesgos a los cuales puede estar expuesta.

- El proyecto “CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA INFORMÁTICA presentado a la UNIVERSIDAD CARLOS III DE MADRID el 23 de Noviembre de 2009, por Esmeralda Guindel Sánchez.

Este proyecto sirve como guía ya que muestra los diferentes tipos de auditoria y cada una de sus fases para su desarrollo y la metodología de trabajo para la aplicación de la auditoria en una empresa, además resalta los errores más comunes en dichas auditorias lo cual es muy importante conocer para evitar incurrir en los mismos errores.

6.2. MARCO CONTEXTUAL

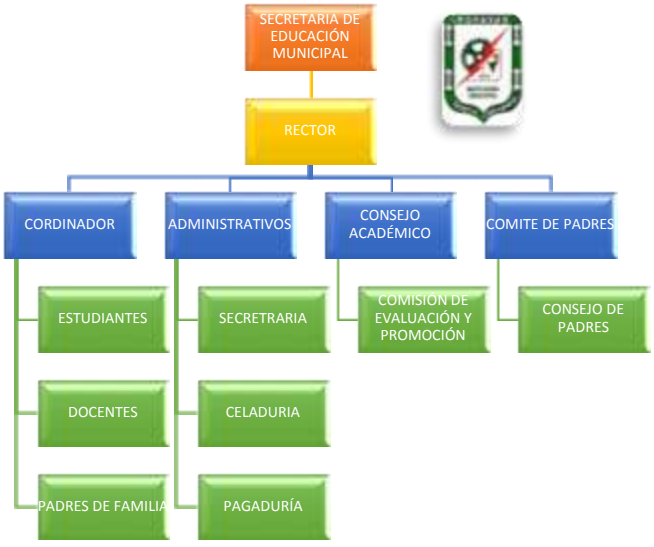
6.2.1. Reseña Histórica

La Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, de carácter oficial y mixto con 52 años de experiencia , comprometida de manera permanente, con el desarrollo social mediante la educación crítica, reflexiva, responsable y creativa dirigida a estudiantes de todos los estratos en los niveles de educación preescolar y básica primaria. Es una institución educativa que forma estudiantes con calidad académica, técnica e investigativa y en valores como; el amor al trabajo y a la educación, respeto ejercicio de la democracia, responsabilidad, sentido de pertenencia, honestidad, con proyección al sector productivo a la educación superior y al desarrollo comunitario.

Forma a personas integras capaces de ingresar a la educación superior, fortaleciendo, habilidades, capacidades y competencias académicas, mediante el conocimiento, adopción y producción de tecnología que contribuyan al progreso social y económico del país.

6.2.2. Organigrama

Figura 1. Organigrama institucional



Fuente: Institución Educativa

- Misión

La Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, de carácter oficial y mixto, comprometida de manera permanente, con el desarrollo social mediante la educación critica, reflexiva, responsable y creativa dirigida a estudiantes de todos los estratos en los niveles de educación preescolar y básica primaria.

Forma a personas integras capaces de ingresar a la educación superior, fortaleciendo, habilidades, capacidades y competencias académicas, mediante el conocimiento, adopción y producción de tecnología que contribuyan al progreso social y económico del país.

- Visión

La Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, será líder en la formación académica, para contribuir a la solución de necesidades regionales y nacionales a través de la articulación con cadenas de formación y alianzas estratégicas con entidades públicas y privadas.

La institución educativa Sede mercedes pardo de Simmonds, ofrece sus servicios educativos a 520 estudiantes, cuenta con equipos tecnológicos de última generación tales como una sala de tecnología e informática dotada de 40 computadores portátiles, 10 computadores de mesa video beam, micrófono inalámbrico, cabina activa, sala de audiovisuales, la institución cuenta con un servicio de internet de 20 Gb.

La institución está conformado por diferentes dependencias que cuentan con el personal necesario e idóneo para la realización de los diferentes procesos académicos y administrativos estas dependencias son:

- Rectoría: el persona de esta dependencia está conformado por dos empleados, que son Rector y Secretaria.
- Coordinación: conformado por Coordinador y secretaria.
- Celaduría: 2 celadores
- Pagaduría: un solo empleado
- Docentes: conformado por 16 docentes
- Estudiantes: 520
- Comité de padres: 5 personas
- Consejo académico: 5 personas

La institución educativa maneja un sistema de información para los procedimientos académicos, como el manejo de calificaciones, creación de logros e indicadores de logro por periodos académicos establecidos por la institución, generación de informes de calificaciones de cada estudiante, información que es creada y modificada por medio de una aplicación web, por medio de perfiles de usuario creados para los docentes, estudiantes, rector, coordinador y secretaria, también maneja información digital y física en los procesos administrativos.

Los procedimientos mencionados anteriormente están enmarcados dentro de del proceso de gestión académica establecida por la institución y que hacen parte del mapa de procesos, entonces a la gestión académica se le realizará un diagnóstico del estado actual de la seguridad de la información haciendo una revisión basado en la norma ISO 27001:2013, realizando una declaración de aplicabilidad de los controles establecido en el Anexo A de la norma en mención y las respectivas recomendaciones para la institución.

6.3. MARCO TEÓRICO

Debido al crecimiento avanzado de las tecnologías de la información en la actualidad se puede indicar que estas son la base fundamental en la realización de actividades en los diferentes entornos como la salud, la educación, el comercio, el transporte entre otros, pero también ha dado lugar a diversos conflictos ya que está expuesto a múltiples ataques que ponen en riesgo la seguridad de la información de las organizaciones, es en este punto donde la seguridad de la información entra a jugar un papel indispensable ya que existe la necesidad de identificar las fallas que se presentan día a día en los sistemas de información y poder dimensionar las posibles soluciones que permitan proporcionar guías, normas y controles para mitigar dichos conflictos y el impacto causado en el riesgo que corren las organizaciones desde diversas perspectivas y que permitan garantizar la integridad de los sistemas de información.

6.3.1 Seguridad de la información**:** El objetivo principal de la seguridad de la información es la protección de los datos con el fin de evitar la pérdida, modificación o divulgación no autorizada de la información ya que estos sucesos ocasionan pérdidas significativas en las organizaciones en los procesos administrativos, operativos, afectando directamente la economía de las organizaciones, motivo por el cual se deben implementar medidas de protección que garanticen la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.

6.3.1.1. Confidencialidad: Este principio tiene como finalidad prevenir la divulgación no autorizada de la información de una organización, garantizando la identificación de las personas que acceden a la información.

6.3.1.2. Integridad: El objetivo principal es preservar los datos de las posibles modificaciones no autorizadas de la información, cuando se habla de integridad de los datos se hace referencia al volumen de los datos y a la fuente de los datos garantizando que no se haya realizado ninguna alteración.

6.3.1.3. Disponibilidad**:** Hace referencia a la disponibilidad de la información cuando los usuarios autorizados lo necesiten y los controles necesarios para prevenir los ataques a la información como la denegación del servicio.

6.3.1.4. Seguridad informática: Es el área que se encarga de implementar, procedimientos, normas, técnicas y métodos para proteger los elementos de un sistema de información minimizando las vulnerabilidades, amenazas, riegos y los impactos que causan.

6.3.2. Vulnerabilidad: Los sistemas informáticos en las organizaciones presentan múltiples vulnerabilidades que son debilidades que puede presentar un sistema informático y esta debilidad puede ser aprovechada por una amenaza afectando directamente a la organización.

Las vulnerabilidades pueden ocasionarse por diversa fallas, en el diseño de actualización errores, en la codificación, mala ubicación de los dispositivos de los sistemas informáticos, software mal configurado, hardware obsoleto, ausencia de copias de seguridad, falta de seguridad en archivos digitales, falta de documentación de las operaciones de las aplicaciones.

6.3.3. Vulnerabilidad Física: Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema.

Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.

6.3.4. Vulnerabilidad Natural: Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.

Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo no disponer de reguladores, no-breaks, mal sistema de ventilación o calefacción, etc.

6.3.5. Vulnerabilidad Hardware: Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

6.3.6. Vulnerabilidad Software: Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.).

Ambos factores hacen susceptible al sistema a las amenazas de software.

6.3.7. Red: Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio.

Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

6.3.8. Factor humano**:** Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema.

Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo.[1]

[1] *Amenazas y vulnerabilidades*. (s.f.). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

6.3.9. Amenazas: Las amenazas se presentan a partir de una vulnerabilidad encontrada en un sistema de información y que pueda ser aprovechada dentro de las amenazas tenemos las amenazas lógicas, amenazas físicas, otras amenazas pueden ser las fallas humanas, las amenazas más conocidas son:

El virus informático: su objetivo es alterar el funcionamiento de un computador sin el permiso del usuario ocasionando diversos problemas como pérdida de la productividad, daños a nivel de datos y cortes en los sistemas.

Los spyware o programas espías: son aplicaciones que recopilan información de un usuario o de una organización sin consentimiento de ellos.

Caballos de Troya: es un programa que puede alojarse en el computador y permite el acceso a usuarios externos que pueden controlar el equipo de forma remota.

6.3.10. Amenazas de Personas: Personal (se pasa por alto el hecho de la persona de la organización incluso a la persona ajeno a la estructura informática, puede comprometer la seguridad de los equipos)

- Ex-emplea dos(generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran en la organización)
- Curiosos (son los atacantes juntos con los crakers los que más se dan en un sistema)
- Hackers (una persona que intenta tener acceso no autorizado a los recursos de la red con intención maliciosa aunque no siempre tiende a ser esa su finalidad)
- Crackers(es un término más preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa)
- Intrusos remunerados (se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son

pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la organización)

6.3.11. Amenazas lógicas: Software incorrecto (a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.).

- Herramientas de seguridad: cualquier herramienta de seguridad representa un arma de doble filo de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos, herramientas como NESUS, SAINT o SATAN pasa de ser útiles a peligrosas cuando la utilizan Crakers.).

- Puertas traseras: durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se está diseñando. Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial.
- Canales cubiertos: son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.

- Virus: un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a sí mismo en otros programas.

- Gusanos: es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos a ser difíciles de programar su número no es muy elevado pero el daño que causa es muy grave.

- Caballos de Troya: son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de él pero que realmente ejecuta funciones ocultas. Programas conejo o bacterias, bajo este nombre se conoce a este programa que no hace nada útil si no que simplemente se delimitan a reproducirse hasta que el número

de copias acaba con los recursos del sistema produciendo una negación del servicio.

6.3.12. Amenazas Físicas**:** Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales.[2]
6.3.13. Riesgos: El riesgo es entonces la materialización de una amenaza, Existen diferentes tipos de riesgo como:

- Riesgo de integridad: que hacen referencia a la autorización y exactitud de la entrada, el procesamiento y el reporte de las aplicaciones, que se hacen presente en el interface del usuario relacionados con la autorización para ejecutar diferentes funciones en la organización, también en la información por la dirección inadecuada de controles que involucran la seguridad de la información que es procesada, a través de la interface también es un riesgo ya que permite que la información sea transferida a otras aplicaciones.

- Riesgos de acceso: Son los riegos del uso no apropiado a los datos e información y al acceso de sistemas comprometiendo la integridad y la confidencialidad de la información de los sistemas y de las bases de datos, estos pueden presentarse en los diferentes niveles de estructura de la seguridad de la información como en la administración de la información, en el entorno de procesamiento, en las redes y a nivel físico.

- Riegos de infraestructura: Cuando en las organizaciones no existe una estructura de información idónea en donde cada uno de sus componentes como el software, redes, hardware, procesos y personas y que no estén en capacidad de soportar las necesidades futuras que se presente dicha organización.

De acuerdo a los las vulnerabilidades, amenazas y riegos es importante que las organización tengan en cuenta la seguridad de la información y el costo que esta tiene pero que también puedan dimensionar que los problemas causados por la falta de seguridad de la información tienen un costo más elevado.

[2] *Seguridad Informática*. (s.f.). Obtenido de https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

6.3.14. ISO 270001; 2013: Para comenzar, se realizaron cambios en su contenido, agregando y eliminando controles, reestructurando especialmente el Anexo “A” donde se aumenta a 14 los dominios de control y se reduce en 20 la cantidad de controles quedando en 113.

Esta nueva versión de ISO/IEC 27001:2013 se adapta con una serie de lineamientos que sirven para el desarrollo de un sistema de gestión de la seguridad de la información, que sin importar el tipo de empresa, se pueda alinear con otros sistemas de gestión en la empresa. Esta nueva estructura propuesta, alineada con el ciclo de la Mejora Continua tiene la siguiente estructura:

- Estructura ISO 27001:2013

En los primeros tres capítulos de este nuevo estándar, ya no aparece la sección “Enfoque del proceso” que contenía la versión anterior y que describía el ciclo PHVA. Además se define el alcance que tiene la normativa para poder certificar, centrándose en los requisitos cubiertos en los capítulos 4 a 10, y si bien ISO-27002 deja de ser una referencia normativa aún es necesaria para implementar este estándar.

En el capítulo 4 Contexto de la organización se resalta la necesidad de hacer un análisis para identificar los problemas externos e internos que rodean a la organización. De esta forma se puede establecer el contexto del SGSI incluyendo las partes interesadas y que deben estar en el alcance del SGSI. En el capítulo 5 Liderazgo, se definen las responsabilidades de la Alta Dirección respecto al SGSI, principalmente en aquellas que demuestren su compromiso, como la definición de la política de seguridad de la información alineada a los objetivos del negocio y la asignación de los recursos necesarios para la implementación del sistema.

Dentro del capítulo 6 Planeación, se prioriza la definición de objetivos de seguridad claros que permita relacionar planes específicos asociados a su cumplimiento. Dentro de la evaluación de riesgos el enfoque se orienta hacia la identificación de aquellos riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, donde el nivel de riesgo aceptable se debe definir en función de la probabilidad de ocurrencia del riesgo y las consecuencias generadas en caso de que este llegara a materializarse (impacto). Y en el capítulo 7 Soporte se relacionan los requerimientos para implementar el SGSI incluyendo recursos, personas y el elemento de comunicación para las partes interesadas en el sistema.

Dentro de los capítulos 4 al 7 se enmarca la etapa de Planeación del sistema. El capítulo 8 Operación, se asocia a la etapa Hacer del ciclo de mejora continua y se establecen los mecanismos para planear y controlar las operaciones y requerimientos de seguridad, en donde las evaluaciones de riesgos periódicas

son el enfoque central para la gestión del sistema. En cuanto a los activos de información, las vulnerabilidades y las amenazas se utilizan para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

El capítulo 9 Evaluación del desempeño se definen las bases para medir la efectividad y desempeño del sistema de gestión a través de las auditorías internas y otras revisiones del SGSI, que plantean planes de acción que permitan atender y solucionar las no-conformidades. Finalmente, el capítulo 10 Mejora propone a partir de las no-conformidades identificadas establecer las acciones correctivas más efectivas para solucionarlas y teniendo el control de que no se repitan.

Aunque las actualizaciones no agregan cambios representativos o radicales en la gestión de la seguridad de la información, estas si incluyen otros conceptos y enfoques que mejoran y facilitan la implementación, de igual forma permiten adaptarse a la evolución de la tecnología y enfocar los esfuerzos en lograr la actualización exitosa. [3]

6.3.15. Metodología Magerit: Esta metodología consiste en la clasificación de activos de la organización en diversos grupos que permitan identificar minuciosamente los riesgos que presenta cada uno y poder temar los controle necesarios, los objetivos de esta metodología es ofrecer un método sistemático que permita analizar los riesgos, planificar las medidas optimas y necesarias para que los riesgos estén bajo control y preparar a la organización para los procesos de evaluación y de auditoria.

Los pasos del método Magerit para el análisis de riesgos son:

- Identificación de activos: que hace referencia a todos los recursos del sistema de información en una organización, que son clasificados de acuerdo a sus características y su jerarquía ya que los activos según su tipo son diferentes las amenazas y salvaguardas para cada uno.
  Dentro de ellos están los siguientes.

  Activos esenciales: En un sistema de información hay 2 cosas esenciales:
  La información que se maneja y los servicios que prestan.
  Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

[3] *IS0 27001; 2013*. (s.f.). Obtenido de http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como, si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos.

Arquitectura del sistema (ARCH): Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.

Datos / Información: Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Claves criptográficas: Las criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

Software - Aplicaciones informáticas: Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

Equipamiento informático (hardware): Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Redes de comunicaciones: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

> Soportes de información: En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Equipamiento auxiliar: En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Instalaciones: En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

Personal: En este epígrafe aparecen las personas relacionadas con los sistemas de información.[4]

- Valoración de activos: es necesario en las organizaciones realizar la valoración de los activos, que no hace referencia al costo de ellos sino el valor que tiene cada activo para las organizaciones, ya que a mayor valor del activo este debe tener mayor protección. La valoración está dada en dimensiones que se clasifican de la siguiente manera:
    - disponibilidad: en donde se evalúa el caso de que el activo no estuviera disponible y su consecuencia si esto sucediera, siendo la disponibilidad una característica que afecta a todos los activos de una organización.
    - integridad de los datos: hace referencia a la situación en el que los datos sean alterados intencionadamente valorando el daño que causaría a la organización en sus diferentes procesos.
    - confidencialidad de la información :

6.3.16. Auditoria: Es una evaluación detallada que se realiza a los sistemas de información de una organización cuyo objetivo es detectar los errores, amenazas, vulnerabilidades y riesgos a los que está expuesta y los resultados son presentados mediante un informe en donde además se establecen las medidas preventivas para corregir dichos riegos y que permitan optimizar la seguridad del sistema de información de la organización.

6.3.17. Auditoria interna :Esta tiene como objetivo principal realizar un control permanente y eficaz en las organizaciones en donde se evalúa las políticas, medidas y procedimientos establecidos por la organización con el fin de proteger los activos, minimizar los riegos y posibles fraudes, optimizar la calidad y seguridad de la información e incrementar la eficacia operativa, direccionando el cumplimiento de las responsabilidades asignadas y posibilitando análisis objetivos, evaluaciones y medidas sobre las operaciones analizadas a los controles operativos, financieros y contables.

[4] Dirección General de Modernización Administrativa, P. e. (Octubre de 2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II.* Madrid: © Ministerio de Hacienda y Administraciones Pública.

6.3.18. Auditoria externa: Se encarga evaluar de forma sistemática las herramientas que soportan la gestión de la organización y todos los procesos que esta realiza con el fin de pronosticar e identificar la integridad del sistema de información administrativo y contable.

6.3.19. Auditoria informática: es un proceso compuesto por diversas fases en donde se realiza recolección y evaluación de evidencias que permiten determinar si un sistema informático y de información cuenta con la seguridad necesaria para proteger todos los activos de la organización, conserva la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

- Objetivos de protección de activos e integridad de datos.

Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas[5] .
Teniendo en cuenta que la información se ha convertido en unos de los activos más importantes de una organización La auditoría informática cumple un papel importante, ya que permite evaluar el sistema de gestión de la información mediante un análisis que se realiza a la organización a través de diversas técnicas y herramientas con el fin de recolectar y agrupar las evidencias según los objetivos propuestos en dicha auditoria, buscando que estos hallazgos puedan ser controlados de forma eficiente.

La auditoría informática tiene objetivos primordiales tales como; la gestión para el cumplimiento de las metas trazadas por la organización, generar una buena relación costo beneficio de los sistemas de información, optimizar la satisfacción de los usuarios del sistema, minimizar los riegos presentes en la organización y la educación y capacitación de los controles en el sistema para la organización, todo ello con el fin de poder obtener un buen desempeño de los sistemas de información que hacen parte de ella , proporcionando los controles adecuados

[5] *Auditoria informática*. (s.f.). Obtenido de https://www.codejobs.biz/es/blog/2013/02/25/que-es-una-auditoria-informatica

para que los sistemas tengan un alto nivel de seguridad y que sea confiable en todos sus aspectos relacionados con en el sistema informático y de información.

6.3.20. Fases de la auditoria: dentro de auditoria se realizan diferentes fases las cuales se explican a continuación.

6.3.20.1. Planeación: Esta fase es primordial ya que si se carece de esta se puede afectar el cumplimiento de la auditoria, permite realizar en primera instancia el conocimiento y comprensión de la organización que va a ser auditada, además se identifica el alcance de la auditoria y sus objetivos principales, esta fase cuenta con unos elementos principales para su desarrollo estos son:

Conocimiento y comprensión de la identidad: se realiza un análisis de la organización en donde se pueden aplicar diferentes técnicas como entrevistas, encuestas, análisis causa- efecto, árbol de problemas, árbol de objetivos entre otros, que permitan conocer la organización que va a hacer auditada de forma detallada, en primera instancia se debe identificar su estructura organizacional, su organigrama en donde se da a conocer la estructura general de la organización, los departamentos que lo conforman y la función de cada departamento, además en este proceso de revisión del organigrama se verifica el cumplimiento de las relaciones funcionales y de tipo jerárquico, de igual manera se comprueba los nombres de los nombres de los puestos de trabajo corresponden a las funciones reales destinadas, políticas y aspectos legales.
Es necesario realizar una investigación de la información de cada una de las áreas que serán auditadas en donde se pueda establecer los objetivos y alcances de cada área, sus recursos materiales y técnicos, el personal de dicha área con sus funciones y los sistemas de información que maneja.

Los encargados de la auditoria deben referenciarse del sitio en el van a desarrollar la auditoria entre ellos la situación geográfica de los sistemas y directos responsables, al igual que la arquitectura y la configuración del hardware y software en cuanto a la distribución de los diferentes equipos y la forma en la que están interconectados, verificando que es un sistema compatible con una configuración adecuada de acuerdo a las políticas de seguridad.
Además deben conocer el inventario hardware y software de la organización en donde se listen los elementos físicos y lógicos que hacen parte del sistema que se va a auditar.

Objetivos y alcance de la auditoria: En donde se identifica el propósito de la auditoria y de esta forma poder determinar también el alcance en donde se especifica las partes de la organización que van a ser examinadas y el tiempo requerido , por ello es de vital importancia que los encargados de la auditoria puedan establecer de forma correcta los objetivos y para ello como primera

medida se debe identificar la actividad de la organización y el área o las áreas más comprometidas en los procesos de la organización de las que se pueda obtener la mejor evidencia y que puedan apoyar los objetivos de la auditoria y de esta forma poder determinar también el alcance, en donde se especifica las partes de la organización que van a ser examinadas y el tiempo requerido para ello.

El alcance de auditoria está directamente relacionado con los objetivos y en la auditoria informática de acuerdo a la organización y a su necesidad pueden existir diversos objetivos algunos de ellos podría ser la confirmación de que los sistemas estén representado de forma precisa y apropiada el capital de la organización, la validación de la exactitud de los sistemas, la evaluación de un proceso realizado en la organización, verificación de la confidencialidad de la información y que esta no este expuesta ya que representa un riesgo alto para la organización y teniendo en cuenta que la información es uno de los activos más importantes en todas las organizaciones.

6.3.20.2. Planes y programas de la auditoria: Después de haber realizado el conocimiento de la organización y cada una de las partes que la componen y de acuerdo al alcance y los objetivos planteados en la auditoria se procede a realizar como primera medida la determinación de los recursos humanos materiales que se necesitaran para la auditoria, dentro de los recursos materiales se debe especificar el software entre ellos los paquetes de auditoria requeridos por el equipo auditor, el hardware ; los computadores, líneas de comunicación e impresoras, estos recursos son facilitados por parte del cliente ya que todos los procesos y pruebas realizadas a la organización deben hacerse en los equipos que hacen parte de esta.

Los recursos humanos en donde se describe el perfil del personal y las competencias que este posee. Entre los perfiles usados para la auditoria informática están;

- Expertos en BD y su administración: quienes deben tener experiencia en manejo y mantenimiento en bases de datos y de diferentes productos.
- Experto en desarrollo de proyectos: cuyas competencias debe ser la capacidad de análisis, conocimiento de las metodologías de desarrollo y con experiencia en desarrollo de proyectos.
- Informático general: quien debe tener capacidad de análisis diseño y gestión de sistemas computacionales en diversas áreas y generador de soluciones tecnológicas que permitan integrar y adaptar sistemas nuevos y existentes,
- Técnico en sistemas: quien debe tener la habilidad de diseñar y realizar mantenimiento preventivo y correctivo a las computadoras, y también organización en procedimientos relacionados con la implementación de diferentes sistemas de información.

Posteriormente se realiza un calendario de actividades que debe ser aprobado por las personas responsables de cada dependencia de la organización y los responsables de la auditoria.

6.3.20.3. Identificación y selección de herramientas, instrumentos y procedimientos: en este punto se diseñan los programas y métodos para la realización de pruebas en donde se establece una guía de la auditoria de todos los procesos a realizar, la identificación se realiza de acuerdo a los objetivos planteados en la auditoria y lo que se busca en ella, entre los procedimientos realizados en la auditoria informática encontramos los siguientes:

- Análisis de datos: en todas las organizaciones cuando se realiza una auditoria informática es necesario verificar y comprobar en conjunto de datos que hacen parte de la organización, para ello se puede usar la comparación de programas en donde se realiza una comparación de código ya sea a los comandos de procesos o al código fuente, entre el programa de ejecución y la versión del programa que previamente ha sido modificado con el fin de encontrar las diferencias.

  Dentro del análisis de datos también se encuentra los datos de prueba cuya finalidad es la verificación de los procedimientos de control de los programas y que estos estén funcionando adecuadamente en donde se prueba realizando diferentes procedimientos con datos correctos y con datos erróneos.

- El proceso de monitoreo también se puede realizar en una auditoria informática siempre y cuando este contemplado dentro de los objetivos, este procedimiento consiste en la evaluación de los procesos de una organización a través del tiempo para verificar si posee algunas necesidades de confidencialidad , integridad y control, dentro del proceso de monitoreo se encuentran los siguientes:

M1 monitoreo del proceso: para llevar a cabo este monitoreo se debe en primera instancia definir los reportes e indicadores de desempeño de los procesos de la organización, establecidos por la gerencia.

M2 evaluar lo adecuado del control interno: este monitoreo se realiza para analizar la efectividad de los controles internos establecidos, dicho monitoreo se realiza por medio de comparaciones, supervisión y poder emitir reportes en continuidad de acuerdo al tiempo estipulado por la organización.

M3 obtención de aseguramiento independiente: es un monitoreo se hace con la finalidad de crear un mejor nivel de confianza entre la organización y los proveedores y los nuevos servicios adquiridos para los cuales se debe realizar una acreditación independiente al igual que un control interno, para poder evaluar la efectividad de forma periódica de los nuevos servicios adquiridos .

Para la auditoria informática hay diferentes pruebas que se pueden aplicar y estas son:

- Pruebas sustantivas: permiten que el auditor informático obtenga las evidencias necesarias por medio de herramientas como entrevistas, muestreos, cálculos, revisiones.

- Pruebas clásicas: la realización de estas pruebas permiten analizar la entrada, la salida esperada y la salida obtenida de los datos de prueba realizados a las aplicaciones o sistemas.

- Pruebas de cumplimiento: estas pruebas consisten en determinar si funciona correctamente el sistema de control interno de la organización En este punto se diseñan los programas y métodos para la realización de pruebas en donde se establece una guía de la auditoria de todos los procesos a realizar.

6.3.20.4. Ejecución de la auditoria: Se realizan los diferentes tipos de pruebas y actividades programadas anteriormente en la etapa de planeación con el fin de evaluar los resultados e identificar los hallazgos, con las evidencias pertinentes que pueden ser físicas, documentales o analítica.

6.3.20.5. Informe final: es el resultado de los estudios, investigación y análisis realizados en cada una de las actividades que han sido ejecutadas en la auditoria de acuerdo a los objetivos establecidos, expresado en un documento final que contiene los hallazgos y las recomendaciones adecuadas.

Este informe final debe expresar la calidad del trabajo realizado en la auditoria y el lenguaje usado debe ser lo más explícito posible usando un lenguaje sencillo y no muy técnico, teniendo en cuenta que las personas a quien se le presenta dicho informe no tienen un alto conocimiento en esta área, el informe debe ser claro, efectivo, confiable, asertivo y exacto.
El informe final de la auditoria tiene una estructura formal, en el cual después de la fecha deben ir especificados los nombres de los auditores y de las personas entrevistadas, en la parte siguiente deben ir los objetivos y el alcance planteado en la auditoria.

También se debe presentar la situación actual de la organización, los puntos débiles y las amenazas encontradas con sus respectivas evidencias, las consecuencias y repercusión de dichas amenazas en los procesos de la organización, las conclusiones, recomendaciones y planes de contingencia requeridos para la organización.

6.3.21. Técnicas y herramientas para la auditoria informática: Cuando se mencionan las técnicas de la auditoria informática, hacemos referencia a los diferentes procedimientos que se realizan en el desarrollo de la auditoria,

mientras que las herramientas hacen parte del conjunto de elementos que permiten el desempeño de las actividades propuestas en las técnicas de la auditoria.

Dentro de las técnicas encontramos las siguientes

- Inspección: Con esta técnica se puede evaluar la eficiencia y la eficacia de un sistema en sus procesamientos y operaciones lo que permite mitigar los riesgos con la evaluación realizada al sistema que es realizada con las características específicas que requiere el sistema y el área de la organización que se está auditando.

- Evaluación: Con dicha técnica se analiza de forma minuciosa y se pone a prueba el cumplimiento de las funciones y operaciones realizadas en una organización, los planes, registros, presupuestos , controles y todo aquello que pueda impedir la administración y el control de dicha organización, con el fin de verificar los diferentes procesos que en ella se realiza.

- Comparación: Mediante esta técnica se realiza una comparación de datos tomados de las áreas auditadas en la organización con el fin de comparar los datos obtenidos con la información de otra organización cuya característica principal es que similar a la organización que se está auditando , en cuanto a los sistemas de información se hace una comparación que consta de los resultados arrojados por el sistema y los resultados arrojados por el proceso manual, dicha comparación es necesaria para saber si la información coincide o tiene alguna falla o desvíos que impidan el cumplimiento de los objetivos que posee la organización.

- Confirmación: Su objetivo principal es corroborar la veracidad de los datos de los sistemas informáticos o de información en sus diferentes procesos que han sido obtenidos de forma directa por los encargados de ejecutar las operaciones involucradas en la verificación.

- Revisión documental: Con esta técnica se hace una revisión detallada de los documentos formales que registra una organización en los diferentes procesos y activadas que se realizan en ella y que de esta manera el auditor comprenda tenga la información exacta sobre el desarrollo de cada uno de los procesos realizados y la comprensión de ellos en donde además se analiza no solo funciones y procedimientos, también se revisan los instructivos o manuales, normas, acuerdos y políticas.

Algunas de las herramientas usadas para la auditoria informática son:

Cuestionarios: En la auditoria informática uno de los objetivos que tiene el auditor es la recolección de la información necesaria sobre la organización y de las áreas que van a ser auditadas para poder de esta manera dar un informe final basado

en las evidencias arrojadas en el desarrollo de la auditoria, para ello una herramienta de gran utilidad es la elaboración y aplicación de cuestionarios que se realizan de acuerdo a la organización y al objetivo de la auditoria, dichos cuestionarios son presentados de forma impresa en formatos las formulaciones de diferentes preguntas sobre el sistema informático y de información de la organización, en donde el auditado responde de acuerdo a su conocimiento y criterio, con la información recolectada en estos cuestionaros el auditor la debe clasificar y analizar por medio de la tabulación.

Entrevistas: Esta herramienta es un medio directo para la recolección de información con la que cuenta el auditor en donde realiza una interrogación e investigación sobre los temas de interés para el desarrollo de la auditoria, para realizar las entrevistas el auditor debe usar una guía general para que se tomen los temas necesarios para poder profundizar en ellos, la evidencia de la recolección de información mediante esta herramienta se debe hacer a través de grabaciones digitales.

Checklist : También denominadas listas de control o listas de chequeo, que son formatos creados con el fin de controlar el cumplimiento de una lista de requisitos de acuerdo a los estándares establecidos para la seguridad de sistema informático y de información de la organización, en cuanto a los procedimientos, el cumplimiento de especificaciones.

6.4. MARCO CONCEPTUAL

6.4.1. Vulnerabilidades: Son debilidades que posee un sistema de información las cuales podrían causar un daño significativo en el sistema en caso de que dicha vulnerabilidad sea explotada, entonces podemos decir que una vulnerabilidad se refleja en la deficiencia en el diseño como por ejemplo en las políticas de seguridad , en el diseño de protocolos, deficiencia en la implementación que hace referencia a errores de programación, existencia de puertas traseras en los sistemas informáticos, o deficiencia en la operación y uso de algún proceso dentro del sistema, entre ellos tenemos la mala configuración de los sistemas informáticos, falta de sensibilización de los usuarios y responsables del sistema, disponibilidad de herramientas que facilitan los ataques.

6.4.2. Amenazas**:** Hacen referencia a los eventos que comprometen la integridad disponibilidad y confidencialidad de la información en donde se puede presentar la oportunidad de atacar el sistema de información de una organización generando daños de acuerdo al nivel de vulnerabilidad presentado, dichas amenazas pueden ser físicas en fallos de hardware, software maliciosos, destrucción, modificación o robo de la información. Dichas amenazas también pueden ser de interrupción en donde se inhabilita el acceso a la información por

medio de la saturación de canales de comunicación, el bloque de acceso a los usuarios o por el daño de componentes físicos, además se encuentran las amenazas de interceptación en donde es captada la información confidencial de la información por medio de personas o programas no autorizados. La amenaza de modificación que va en contra del principio de integridad de los datos al ser estos modificados sin autorización.

6.4.3. Riesgo **:** Es la materialización de una amenaza aprovechando la vulnerabilidad presente en la organización en donde existe la probabilidad de pérdida o daño en una organización y este es cuantificable evidenciando el impacto que este causaría si ocurriera , es por ello que es de vital importancia para las organizaciones identificar los riesgos existente como su probabilidad e impacto con el fin de mitigar la materialización de estos, realizando un análisis y evaluación que permitan valorarlos , tratarlos, transferirlos o aceptarlos a través de la gestión de riesgos indicando los controles y medidas de seguridad aplicadas

6.4.4. Probabilidad de ocurrencia: Cuando los riegos ya han sido identificados se realiza un análisis minucioso que permite clasificar los riesgos menores o aceptables de los mayores e inminentes donde además se analiza la posibilidad de ocurrencia o frecuencia del riesgo y su factibilidad teniendo en cuenta los factores internos y externos.

6.5. MARCO LEGAL

El proceso de auditoría a una organización está estrechamente ligado con el cumplimiento de las leyes, decretos y estándares necesarios incluyendo la ética profesional de los auditores los cuales se deben regir a los códigos de ética establecidos de acuerdo a su profesión, en pro de salvaguardar los activos que hacen parte de la organización y poder brindar un trabajo de calidad basado en las leyes vigentes que son:

"*LEY 527 DE 1999 (agosto 18) por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."*[6]

"Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información

[6]*Ley 527 de 1999*. (s.f.). Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".[7]

"*DECRETO 1747 DE 2000 (septiembre 11), por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales"*[8]

"*LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008 por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."*[9]

[7] *Ley 1273 de 2009*. (s.f.). Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3705.html

[8] *Decreto 1747* . (s.f.). Obtenido de: http://www.sic.gov.co/drupal/recursos_user/historico/d2011sic967.html

[9] *Ley estatutaria 1266*. (s.f.). Obtenido de https://www.uiaf.gov.co/?idcategoria=20630

7. MARCO METODOLÓGICO

7.1. METODOLOGÍA DE INVESTIGACIÓN :

El presente proyecto se basó en el análisis cualitativo de la organización mediante el diagnóstico de la seguridad de la información aplicado al proceso gestión académica, el análisis se basó en la norma ISO 27001: 2013 para la identificación de las amenazas, vulnerabilidades y riesgos, la probabilidad de ocurrencia y el impacto en caso de materialización.

7.1.1. Tipo de investigación**:** Investigación aplicada tiene como objetivo principal, la solución de problemas puntuales que permiten mejorar la calidad de vida en un entorno determinado.

"Investigación básica, se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación aplicada busca el conocer para hacer, para actuar, para construir, para modificar*"*[10]

al realizar una investigación para la institución educativa se busca en primera instancia conocer su funcionamiento general, que permita tener una visión macro de los procesos realizados y poder enfocarse posteriormente en el conocimiento específico y detallado del proceso gestión académica que fue el seleccionado para el desarrollo del presente proyecto; una vez reconocido los procedimientos realizados en el proceso de gestión académica se hace un análisis de la información recolectada que permita hacer una evaluación de riesgos y poder realizar un diagnóstico a la seguridad de la información basada en la norma ISO 27001:2013, con el fin de disminuir el impacto y probabilidad de ocurrencia de vulnerabilidades, amenazas y riesgos a la que está expuesta la institución Educativa Sede Mercedes Pardo de Simmonds de la ciudad de Popayán y de esta manera poder presentar los controles adecuados y su debidas recomendaciones al proceso seleccionado.

[10] (Tipos de investigación , s.f.)http://biblioteca.uns.edu.pe/saladocentes/archivoz/curzoz/002_clase4.pdf

7.2. METODOLOGÍA DE DESARROLLO

7.2.1. Recolección de información e identificación de procesos de la institución. Se inició con la fase de levantamiento de información de la organización que permitió conocer de forma precisa los procesos realizados en la institución, en esta primera etapa se aplicaron las siguientes técnicas de recolección:

Observación: se realizó una visita a las instalaciones de la Institución, con el objetivo de conocer la ubicación y condiciones de los componentes que intervienen en los procesos, mediante registros fotográficos sobre la visita.

Entrevista estructurada: se realizaron dos entrevistas diferentes, una que permitía conocer los activos que la institución posee y otra entrevista para los actores principales de los proceso gestión académica, estos actores han sido previamente identificados, las entrevistas contenían una estructura básica con preguntas de selección múltiple y única respuesta y preguntas cerradas que tienen como respuesta “si” o “no”.

Lista de chequeo**:** se hizo con el fin de realizar una identificación, análisis y verificación si existen o no controles de seguridad en la institución para el proceso de gestión académica, además identificar la seguridad para los usuarios del sistema, seguridad en los accesos al sistema de información, seguridad de los activos en la institución, administración del sistema que hacen parte del proceso de gestión académica.

Las técnicas de recolección de información antes mencionadas fueron tomadas de fuentes primarias ya que se estableció un contacto directo con los actores principales del proceso de gestión académica de la institución lo que permitió obtener una información precisa para su posterior análisis.

7.2.2. Identificación de procedimientos del proceso gestión académica:

Con el resultado de la información recolectada se logró identificar el mapa de procesos de la institución de forma general y enfocarnos en la descripción detallada del proceso de gestión académica seleccionado en donde reconoció cada uno de los procedimientos realizados dentro del proceso en mención y su respectivo análisis.

7.2.3. Identificación y valoración de activos:

La información recolectada también fue la base para la identificación de activos de la institución , su valoración de los posibles riesgos sus vulnerabilidades y amenazas, así como su probabilidad de ocurrencia y el impacto de los mismos para la seguridad de la información de la institución, este procedimiento se

realizó con el fin de poder hacer una la declaración de aplicabilidad de la norma ISO 27001;2013 usando para ello la metodología Magerit como apoyo para la realización del diagnóstico para la institución , también se presenta el análisis de la aplicación web libreta escolar para reconocer sus fallas a nivel de seguridad de la información en dicho procedimiento.

7.2.4. Declaración de aplicabilidad (SOA) Norma ISO 27001;2013

De acuerdo a la información recolectada y a su análisis se realizó una matriz basada en la Norma ISO 27001;2013 denominada declaración de aplicabilidad en donde se revisó los 144 controles estipulados en la norma y se eligieron los que aplican para la institución en el proceso de gestión académica en donde se justificó su elección y se identificó que controles no se están cumpliendo, además se sustentó la razón por la cual se excluyen algunos controles que no aplican para la institución.

7.2.5. Diagnostico

Con los controles identificados de acuerdo a la norma ISO 27001;2013 se presenta como producto un diagnóstico a través de un informe sobre el estado actual de la seguridad de la información, en el proceso gestión académica con las observaciones pertinentes para la institución educativa.

7.3. UNIVERSO Y MUESTRA.

El universo muestra del presente proyecto son los cuatro procesos que tiene la Institución Educativa que son: gestión directiva, gestión académica, gestión de bienestar y convivencia, y gestión administrativa.

Después de la identificación de los procesos antes mencionados se utilizó el tipo de muestreo no probabilístico, en el nivel de muestreo por cuotas ya que se va a entrevistar a todos los actores principales del proceso de gestión académica el cual fue seleccionado para su análisis, la recolección de información se hará para los siguientes procedimientos y sus actores principales:

Tabla 1. Muestra de los procedimientos de la gestión académica

PROCEDIMIENTOS	RESPONSABLE
Registro de calificaciones en la aplicación web libreta escolar.	Docentes, coordinador y secretaria
Inscripción de estudiantes nuevos	Secretaria
Matricula de estudiantes nuevos y antiguos	Docentes y secretaria
Registro de estudiantes en el sistema integrado de matrícula Simat	Secretaria
Generación de certificados y constancias de estudio.	Secretaria, coordinador

Fuente : El autor

7.4. FUENTES DE RECOLECCIÓN DE INFORMACIÓN.

En el desarrollo del diagnóstico del estado actual de la seguridad informática de la Institución, se realizó un conocimiento de la organización por medio de diferentes técnicas de recolección de información a las personas encargadas directamente de los procedimientos realizados en el proceso de gestión académica, con el fin de recolectar la información necesaria como objeto de análisis del proceso seleccionado y poder realizar el diagnóstico adecuado a la Institución.

Las fuentes de recolección de información usadas fueron fuentes primarias, las cuales fueron producidas en el presente proyecto mediante las técnicas de recolección de información como los son; la observación, entrevista y lista de chequeo, diseñadas para aplicarlas a las personas implicadas en el proceso de

gestión académica que fue previamente seleccionado, para ello se tuvieron en cuenta los roles de cada persona como se describen a continuación:

Coordinador: debe realizar la asignación académica anualmente para cada docente en la aplicación web, realizar la apertura y cierre del plazo para la codificación de logros y notas para los docentes en la aplicación web, revisión de los borradores de los informes generados por la aplicación web en cada periodo académico, dar el visto bueno para proceder a la firma de informes, certificados y constancias solicitadas.

Docentes: estos actores tienen a cargo el registro de calificaciones en la aplicación web libreta escolar de cada área de acuerdo a la asignación académica realizada al inicio de año, reporte de faltas, y la matrícula de estudiantes antiguos.

Secretaria: está encargada de actualizar la base de datos de los estudiantes en la aplicación web, realizar en dicha aplicación la asignación académica de cada docente anualmente, generar e imprimir los resúmenes de periodo a cada docente, realizar las correcciones respectivas entregadas por los docentes en la aplicación web, hacer Inscripción de estudiantes nuevos, registro de estudiantes en el sistema integrado de matrícula Simat y generación de certificados y constancias de estudio.

8. RECURSOS.

Los recursos que se necesitaron para la realización del presente proyecto para la institución educativa Técnico Industrial Sede Mercedes Pardo fueron; un ingeniero de sistemas que realizará el diagnóstico del estado actual de la seguridad de la información llevando a cabo las fases descritas en el diseño metodológico para lo cual necesitaron algunos insumos como se describen a continuación:

Tabla 2.Recursos y presupuesto

RECURSOS Y PRESUPUESTO		
Recursos	Descripción	Presupuesto
Talento humano	Ingeniero de sistemas	$ 3.500.000
Materiales físicos	Papelería, impresión, carpetas	$ 100.000
Recursos tecnológicos	Computador portátil, cámara digital	$ 2.000.000
Total		$ 5.600.000

Fuente: el autor

9. PRODUCTO

El producto a entregar es un informe que contenga el resultado del análisis de la seguridad de la información en el proceso gestión académica de la institución basada en la norma ISO 27001:2013 en donde se va a definir un diagnostico a través de una declaración de aplicabilidad los controles aplicados a la institución y las recomendaciones respectivas a cada control seleccionado para que la institución tome las medidas necesarias para el tratamiento de riesgos existentes y se pueda minimizar las amenazas identificadas de la seguridad de la información, este se presentara como un informe final.

.

10. DESARROLLO DEL PROYECTO

10.1. Identificación de los procesos de la institución

De acuerdo a la recolección de información y a partir de la visita realizada a la institución educativa, para el reconocimiento general de sus instalaciones y procesos realizados, se logró identificar que la institución actualmente cuenta con un mapa de procesos que describe las diferentes actividades realizadas como se muestra en el siguiente gráfico

figura 2 . Mapa de procesos de la institución

Fuente : El autor

Dentro de los procesos identificados en la institución se selecciona el proceso de gestión académica y por medio de la entrevista realizada a los actores principales de este proceso se puede reconocer que está compuesto por cinco procedimientos que son Inscripción de estudiantes nuevos, matrícula de estudiantes nuevos y antiguos, registro de calificaciones en la aplicación web libreta escolar, Generación de certificados y constancias de estudio, estos procedimientos se describen a continuación:

figura 3 . Proceso gestión académica

Fuente: El autor

Tabla 3. Descripción proceso gestión académica

PROCESO GESTIÓN ACADÉMICA			
PROCEDIMIENTO	**Área RESPONSABLE**	**OBJETIVO**	**DESCRIPCIÓN**
Registro de calificaciones en la aplicación web libreta escolar.	Docentes, coordinador y secretaria	Ingresar y codificar en el sistema los logros de cada área y las calificaciones de cada periodo académico.	En primera instancia la secretaria es la encargada de cargar al sistema la base de datos con los nombres de los estudiantes y el grado que cursan, después procede a la asignación de la carga académica en el sistema, de acuerdo al reporte entregado por parte del coordinador, después se crean las planillas de notas para cada área según la carga académica de los docentes, por ultimo establece las fechas de apertura y cierre del sistema para los usuarios docentes. De acuerdo a un cronograma entregado a los docentes, deben ingresar los logros de al sistema de cada área de acuerdo a la valoración dada a los diferentes desempeño para que estos sean codificados por el sistema, después debe ingresar las calificaciones del área asignada según la carga académica a cada estudiante, generar el resumen de calificaciones para identificar posibles errores y posteriormente generar el borrador de informe final para su revisión de redacción y presentación del informe. La secretaria después de cerrado el sistema para los docentes, genera un resumen de calificaciones que le entrega a los docentes, para revisión de calificaciones, los docentes entregan el resumen con las respectivas correcciones, las secretaria las modifica en el sistema y finalmente procede a la impresión de los boletines.

Tabla 4. (Continuación)

PROCESO GESTIÓN ACADÉMICA			
PROCEDIMIENTO	**Área RESPONSABLE**	**OBJETIVO**	**DESCRIPCIÓN**
Inscripción de estudiantes nuevos	Secretaria	Realizar el proceso de recepción de documentos iniciales a los estudiantes nuevos, de acuerdo a la disponibilidad de cupos trazada en la proyección realizada para el siguiente año académico.	En el área de secretaria se realiza el proceso de inscripción de acuerdo a la disponibilidad de cupo, este proceso permite que el padre de familia separe el cupo del estudiante, los requisitos que se deben entregar son fotocopia del documento de identidad y el último informe académico del estudiante de la institución de donde proviene y el diligenciamiento del formato de inscripción con los datos del estudiante y sus acudientes.
Matricula de estudiantes nuevos y antiguos	Docentes y secretaria	Recibir y revisar los documentos de los estudiantes, solicitados para la matrícula y diligenciar el formato de matrícula.	Los docentes se encargan de realizar la matrícula de los estudiantes antiguos, reciben el informe final del estudiante donde indica el grado al que es promovido, diligencian el formato de matrícula y archivan los documentos en la carpeta del estudiante, después entregan las carpetas de los estudiantes a la secretaria. La secretaria hace el mismo procedimiento de matrícula que los docentes, además se realiza la verificación del retiro del simat en el sistema.

Tabla 5. (Continuación)

PROCESO GESTIÓN ACADÉMICA			
PROCEDIMIENTO	**Área RESPONSABLE**	**OBJETIVO**	**DESCRIPCIÓN**
Registro de estudiantes en el sistema integrado de matrícula Simat	Secretaria	El sistema integrado de matrícula Simat, es un sistema de gestión para las entidades educativas oficiales que permite sistematizar , consolidar y analizar información, mejorando los procesos de inscripción , asignación de cupos y matricula	El sistema integrado de matrícula es dirigido por la secretaria de educación, quienes asignan un cronograma de cumplimiento para los diferentes procesos o etapas de la matrícula, la cual inicia con una proyección de cupos para el año lectivo, inscripción de estudiantes nuevos, pre matricula de estudiantes antiguos, asignación de cupos a estudiantes nuevos, reprobación de estudiantes antiguos y finalmente matricula de estudiantes nuevos y antiguos, retiro de estudiantes y liberación de cupos. La secretaria es la encargada de cumplir con todos los procesos y para su evidencia el sistema permite descargar reportes de cada etapa realizada.
Generación de certificados y constancias de estudio.	Secretaria y coordinador	Cumplir con las solicitudes de certificados y constancias de estudio para estudiantes y egresados.	La secretaria recibe la solicitud del documento que necesita el estudiante y por medio de plantillas diseñadas en la institución en el programa Word, se digita con los datos pertinentes, la secretaria lleva un número de registro para las constancias y certificaciones de forma manual, escrita su secuencia en una agenda personal, la constancia o el certificado es impreso y firmado por el coordinador.

Fuente : el autor.

10.2. IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS

Se le solicitó a la institución información precisa del número de equipos, características, documentación y localización, planes de instalación, planes de mantenimiento, configuración de los equipos y capacidad de estos y las políticas de uso.

Esto se realizó con el fin de tener un conocimiento general y detallados del sistema informático de la institución para poder realizar un diagnóstico de la seguridad información con la que cuenta la institución.

En cuanto a la aplicación web se realizó una verificación de los procedimientos que realiza y las características de cada módulo y las funciones específicas de cada usuario.

Para la identificación de activos que posee la institución se realizó diferentes procesos de recolección de datos, entre ellos una encuesta como lo muestra el anexo A con el fin de conocer el personal de la institución y la planta física, también se realizaron dos listas de chequeo (Anexo C y D), para verificar la seguridad de los equipos y de la información, y también un cuestionario hardware de control e inventario de equipos (Anexo. E) la información recolectada está registrada en las siguientes tablas.

SW: aplicaciones software, HW: equipos informáticos, SI: soporte de información, COM: comunicaciones, EAUX: equipamiento auxiliar, L: Instalación, P: personal

Inventario por dependencias

Dependencia: Coordinación

Tabla 6. Dependencia: Coordinación

Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
1	Computador de mesa hp	Reportes, informes	HW,SW;SI
1	Impresora Epson	Impresiones coordinación	HW
1	Modem	Conexión a internet	HW
1	Archivador	Informes contables y académicos	Media

Fuente: el autor

Tabla 7. Dependencia: Administrativa

Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
2	Computador de mesa hp	Reportes, informes, listados, cotizaciones	HW,SW;SI
1	Impresora Epson multifuncional	Impresiones secretaria	HW
3	Archivador	Informes académicos, documentos de estudiantes constancias	Media

Fuente: el autor

Tabla 8. Dependencia: Docentes

Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
10	Computador de mesa hp	Reportes, informes, listados, calificaciones	HW,SW;SI
1	Impresora Epson	Impresiones Docentes	HW
10	Televisor log plasma	Proyección de videos, imágenes en el aula.	HW

Fuente: el autor

Tabla 9. Dependencia: Sala de informática

Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
40	Computador portátil pc Smart	Uso de estudiantes área tecnología e informática	HW,SW;SI
1	Impresora Epson	Impresiones estudiantes	HW

Tabla 10. (Continuación)

Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
1	Cabina activa Dj pro	Audio sala informática	HW
1	Video beam Lg	Proyecciones sala informática	HW

Fuente: el autor

Tabla 11. Aplicación web

Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
1	Aplicación web www.libretaescolar.com	Registro de calificaciones e informes de periodo	SW

Fuente: el autor

Después de encontrar los datos registrados anteriormente por las encuestas realizadas presentes en el anexo A. Se realizó la siguiente identificación de activos de acuerdo a la metodología Magerit con respaldo del libro 1 y el libro 2

Tabla 12. Identificación de activos

IDENTIFICACIÓN DE ACTIVOS	
Tipo de activo	**Activo**
[D] Datos/Información	[int] datos de gestión interna
	[password] contraseñas ,aplicación web
	[auth] datos de validación de credenciales
	[BACKUP] Copias de respaldo
	[TEST] Datos de prueba
[SW] Software	[BROWSER] Navegador web

Tabla 13. (Continuación)

IDENTIFICACIÓN DE ACTIVOS	
Tipo de activo	**Activo**
[SW] Software	[APP] Aplicación web académico
	[DBMS] Sistema de gestión de bases de datos
	[OFFICE] Ofimática
	[AV] Anti virus
	[OS] Sistema operativo
[HW] Equipamiento informático	[IPPHONE] teléfono
	[PC] Computadores de mesa
	[PC] Computadores portátiles
	[PERIPHERAL] Cabina activa
	[PRINT] Impresora de soporte
	[LAN] Cableado red de área local
	[SWITCH] Switch
[COM] Redes de comunicaciones	[WIFI] red inalámbrica
	[INT] Internet
	[PSTN] Red telefónica
	[LAN] Red local
[Media] Soportes de información	[NON_ELECTRONIC] no electrónicos
	[PRINTED] Material impreso. Constancias, boletines, informes
[AUX] Equipamiento auxiliar	[AC] Equipos de climatización
	[FURNITURE] Mobiliario

Tabla 14. (Continuación)

IDENTIFICACIÓN DE ACTIVOS	
Tipo de activo	**Activo**
[L] Instalaciones	[OFI] Oficina
	[BUILDING] Edificio
	[ADM] Administradores de sistemas
	[UI] Usuarios internos

Fuente: el autor

10.3. VALORACIÓN DE LOS ACTIVOS

Tabla 15. Valoración de activos

NIVEL	CRITERIO
10	Alto
9	Alto
8	Alto
7	Alto
6	Alto
5	Medio
4	Medio
3	Medio
2	Bajo
1	Bajo
0	Depreciable

Fuente: el autor

Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

Tabla 16. Valoración de activos por dimensiones.

VALORACIÓN DE ACTIVOS POR DIMENSIONES					
	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios internos					
Router	[8]			[8]	[8]
Aplicaciones					
Aplicación web académico	[8]			[8]	[7]
Antivirus					[7]
Sistema Operativo					[7]
Sistema de Información	[9]	[9]	[9]	[9]	[9]
Equipos					
Medios de Impresión					[6]
Computadores de escritorio					[8]
Modem					[8]
Computadores portátiles					[8]
Comunicaciones					
Conmutador	[8]	[7]			[7]

Tabla 17. (Continuación)

VALORACIÓN DE ACTIVOS POR DIMENSIONES					
	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Red WIFI					[7]
router		[7]	[7]		
Soportes de Información					
Documentación digital de procesos		[8]	[8]		
Documentación digital del Sistema de Información		[8]	[8]		
Informes en digital y físico		[8]	[8]		
Equipamiento Auxiliar					
Reguladores	[7]				
Antenas USB	[7]				
Instalaciones					
Sede Institución educativa			[8]		
Personal					
Coordinador			[8]		
Docentes			[8]		
Secretaria			[7]		
Pagaduría			[7]		
Celadores			[7]		
Comité de padres			[6]		

Fuente: el autor

10.4. CARACTERIZACIÓN DE LAS AMENAZAS

En este punto se identificarán los tipos de amenaza de acuerdo al libro II margerit en donde se encuentra el catálogo de las amenazas en donde se clasifican en diferentes tipos que son; [N] desastres naturales, [I] de origen industrial, [A] ataques intencionados, [E] errores y fallos no intencionados. Entonces en primera instancia se identifican las amenazas de acuerdo a los tipos anteriormente mencionados y posteriormente se realiza una valorización de dichas amenazas.

Tabla 18 caracterización de amenazas

Activos	Amenazas
Computadores portátiles	[N.2] Daños por agua
	[I.8] Fallo de servicios de comunicaciones
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[I.10] Degradación de los soportes de almacenamiento de la información
	[E.14] Escapes de información.
	[E.23] Errores de mantenimiento, actualización de equipos hardware
	[E.25] Pérdida de equipos
	[A.22] Manipulación de programas.
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.23] Manipulación de los equipos.
Computadores de mesa	[N.2] Daños por agua
	[I.8] Fallo de servicios de comunicaciones

Tabla 12. (Continuación)

Activos	**Amenazas**
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[I.10] Degradación de los soportes de almacenamiento de la información
	[E.14] Escapes de información. [E.23] Errores de mantenimiento, actualización de equipos hardware [E.25] Pérdida de equipos
	[A.22] Manipulación de programas. [A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.23] Manipulación de los equipos.
Sistema de Información	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades del programa (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.7] Uso no previsto
	[A.24] Denegación de servicios
	[A.11] Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
Antivirus	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)

Tabla 12. (Continuación)

Activos	**Amenazas**
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
Sistema Operativo	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.7] Uso no previsto
Aplicación web	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades del programa (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.7] Uso no previsto
	[A.24] Denegación de servicios
	[A.11] Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
Impresoras	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[E.23] Errores de mantenimiento, actualización de equipos hardware
	[A.11] Acceso no autorizado

Tabla 12. (Continuación)

Activos	**Amenazas**
	[N.2] Daños por agua
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[A.11] Acceso no autorizado
	[A.4] Errores de configuración
Telefonía	[A.11] Acceso no autorizado
Red WIFI	[I.4] Fallo de servicios de comunicaciones [E.8] Errores de re-encaminamiento
INTERNET	[I.8] Fallo de servicios de comunicaciones [E.15] Alteración de la información
Documentación digital de procesos.	[A.11] Acceso no autorizado
	[E.15] Alteración de la información
	[A.15] Modificación de la información
	[A.25] Robo de la información
Documentación digital del Sistema de Información.	[A.11] Acceso no autorizado
	[E.15] Alteración de la información
	[A.15] Modificación de la información
	[A.25] Robo de la información
Informes en digital y físico	[A.11] Acceso no autorizado
	[E.15] Alteración de la información
	[A.15] Modificación de la información
	[A.25] Robo de la información

Tabla 12. (Continuación)

Activos	**Amenazas**
Antenas	[I.4] Contaminación electromecánica
Sede institución educativa	[N.1] Fuego
	[N.2] Daños por agua
	[.*] Desastres naturales.
	[A.27] Ocupación enemiga
Rector	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Docentes	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Secretaria	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Pagaduría	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Celadores	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Comité de padres	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social

Fuente: el autor

10.5. VALORACIÓN DE AMENAZAS

En esta etapa se muestra el daño que puede causar una amenaza sobre los tipos de activos si ésta se materializa. La valoración de la amenaza está relacionada con el daño que puede causar a una o varias de las dimensiones de un activo identificado, también se mide su probabilidad, es decir, cuán probable es que la amenaza se materialice. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.[11]

Para la medir el daño o nivel de degradación se usara la siguiente tabla:

Tabla 19 medición daño o nivel de degradación

Valor	Descripción	
100%	MA	Muy alta
80%	A	Alta
50%	M	Media
20%	B	Baja
10%	MB	Muy baja

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método

Tabla 20. Frecuencia

Valor	Descripción		
100	MF	Muy frecuente	A diario
10	F	Frecuente	Mensualmente
1	N	Normal	Una vez al año
1/10	P	Poco	Cada varios años
1/100	MP	Muy poco frecuente	Siglos

[11] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método

El proceso de valoración de activos mediante la metodología Magerit tiene como objetivo cuantificar el daño y lo que este ocasionaría para la organización en el caso que se llegara a materializar la amenaza, afectando los atributos que posee el activo en donde se caracteriza con relación a sus dimensiones.

Las dimensiones que se van a valorar son:

- [D] Disponibilidad: El activo puede ser usado por las entidades o procesos autorizados lo requieran.
- [I] Integridad de los datos: El activo no ha sido alterado por individuos, entidades o procesos no autorizados. Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
- [C] Confidencialidad: Es el aseguramiento de que la información es accesible sólo para aquellos individuos o entidades autorizados.
- [A] Autenticidad: La entidad que accede al activo es quien dice ser.
- [T]Trazabilidad: El acceso a la información protegida y la realización de operaciones debe ser registrada para evitar el repudio por parte de quien lo hace.

Tabla 21. valoración de las amenazas.

Activos	**Amenazas**	**frecuencia**	**D**	**I**	**C**	**A**	**T**
Computadores portátiles	[N.2] Daños por agua	10	90%				25
	[I.8] Fallo de servicios de comunicaciones	10	80%				16
	[I.5] Avería de origen físico o lógico	10	70%				12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	1	10%				4
	[I.10] Degradación de los soportes de almacenamiento de la información	1/10	60%	20%	20%		12

Tabla 15. (Continuación)

Activos	Amenazas	frecuencia	D	I	C	A	T
	[E.14] Escapes de información.	10		90%	90%		25
	[E.23] Errores de mantenimiento, actualización de equipos hardware	10	70%				16
	[E.25] Pérdida de equipos	1/10	60%				16
	[A.22] Manipulación de programas.	100	60%	80%			20
	[A.6] Abuso de privilegios de acceso	10	70%	80%	80%		20
	[A.7] Uso no previsto	10	50%	20%	20%		12
	[A.23] Manipulación de los equipos.	100	80%		60%		16
Computadores de mesa	[N.2] Daños por agua	10	90%				25
	[I.8] Fallo de servicios de comunicaciones	10	70%				16
	[I.5] Avería de origen físico o lógico	1	60%				12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	1	10%				4
	[I.10] Degradación de los soportes de almacenamiento de la información	1/10	50%	40%	60%		12
	[E.14] Escapes de información.	10	80%	90%	70%		25
	[E.23] Errores de mantenimiento, actualización de equipos hardware	10	80%				16
	[E.25] Pérdida de equipos	1/10	70%				16
	[A.22] Manipulación de programas.	100	80%		60%		20
	[A.6] Abuso de privilegios de acceso	10	80%	80%	60%		20

Tabla 15. (Continuación)

Activos	Amenazas	frecuencia	D	I	C	A	T
	[A.7] Uso no previsto	10	50%	60%	50%		12
	[A.23] Manipulación de los equipos.	100	80%		50%		16
	[I.6] suministro eléctrico	1	50%				20
Sistema de Información	[E.1] Errores de los usuarios	10	50%	50%	60%		12
	[E.8] Difusión de software dañino	10	70%	80%	60%		20
	[E.20] Vulnerabilidades del programa (software)	10	60%	50%	70%		12
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	10	80%				20
	[A.7] Uso no previsto	10	40%	50%	50%		12
	[A.24] Denegación de servicios	1	60%	80%	60%		16
	[A.11] Acceso no autorizado	10	80%	70%	80%		20
	[A.6] Abuso de privilegios de acceso	10	90%	90%	80%		25
Antivirus	[E.8] Difusión de software dañino	1	80%	80%	70%		20
	[E.20] Vulnerabilidades de los programas (software)	10	50%	70%	60%		12
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	10	80%				20
Sistema Operativo	[I.5] Avería de origen físico o lógico	1	60%	50%	50%		12
	[E.1] Errores de los usuarios	1	70%	60%	50%		12
	[E.8] Difusión de software dañino	10	80%	70%	80%		16

Tabla 15. (Continuación)

Activos	Amenazas	frecuencia	D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	10	50%	50%	70%		12
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	10	80%				16
	[A.7] Uso no previsto	1	80%				20
Aplicación web	[E.1] Errores de los usuarios	10	80%	70%	60%		16
	[E.8] Difusión de software dañino	1	80%	60%	80%		20
	[E.20] Vulnerabilidades del programa (software)	10	90%	80%	80%		25
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	1	60%				12
	[A.7] Uso no previsto	10	80%				16
	[A.24] Denegación de servicios	1	60%	80%	70%		20
	[A.11] Acceso no autorizado	10	90%	80%	90%		25
	[A.6] Abuso de privilegios de acceso	1	80%	80%	80%		25
Impresoras	[I.5] Avería de origen físico o lógico	10	50%	50%	50%		12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	1/10	10%				4
	[E.23] Errores de mantenimiento, actualización de equipos hardware	1	30%	20%	10%		6
	[A.11] Acceso no autorizado	1	20%	10%	20%		4
Router	[N.1] Fuego	1	30%				6

Tabla 15. (Continuación)

Activos	Amenazas	frecuencia	D	I	C	A	T
Router	[N.2] Daños por agua	1	30%				6
	[I.5] Avería de origen físico o lógico	10	A	M	M		12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	1	A				4
	[A.11] Acceso no autorizado	10	50%	20%	50%		12
	[E.4] Errores de configuración	10	50%	20%	50%		16
Telefonía	[A.11] Acceso no autorizado	10	20%	50%	20%		4
Red WIFI	[I.4] Fallo de servicios de comunicaciones	1	20%	20%	20%		20
	[E.8] Errores de re-encaminamiento	1	20%	20%	20%		12
INTERNET	[I.8] Fallo de servicios de comunicaciones	10	50%	50%	50%		20
	[E.15] Alteración de la información	1	20%	50%	50%		25
Documentación digital de procesos.	[A.11] Acceso no autorizado	10	20%	50%	20%		25
	[E.15] Alteración de la información	1	20%	20%	20%		20
	[A.15] Modificación de la información	1	20%	20%	50%		25
	[A.25] Robo de la información	1	20%	20%	50%		25
Documentación digital del Sistema de Información.	[A.11] Acceso no autorizado	10	20%	50%	20%		20
	[E.15] Alteración de la información	1	20%	20%	20%		20
	[A.15] Modificación de la información	1	20%	20%	50%		20
	[A.25] Robo de la información	1	20%	20%	50%		25
Informes en digital y físico	[A.11] Acceso no autorizado	10	20%	50%	20%		16
	[E.15] Alteración de la información	1	20%	20%	20%		20

Tabla 15. (Continuación)

Activos	Amenazas	frecuencia	D	I	C	A	T
	[A.15] Modificación de la información	1	20%	20%	10%		2
	[A.25] Robo de la información	1	90%	90%	80%		25
Antenas	[I.4] Contaminación electromecánica	1/10	10%				4
Sede institución educativa	[N.1] Fuego	1	30%				6
	[N.2] Daños por agua	1	30%				2
	[.*] Desastres naturales.	1/10	10%				6
	[A.27] Ocupación enemiga	1/10	10%				8
Coordinador	[E.28] indisponibilidad del personal	10	40%				6
	[A.29] Extorsión	1/10	10%	10%	10%		1
	[A.30] Ingeniería Social	1	20%	20%	20%		6
Docentes	[E.28] indisponibilidad del personal	10	40%				6
	[A.29] Extorsión	1/10	10%	10%	10%		1
	[A.30] Ingeniería Social	1	20%	20%	20%		6
Secretaria	[E.28] indisponibilidad del personal	10	40%				6
	[A.29] Extorsión	1/10	10%	10%	10%		1
	[A.30] Ingeniería Social	1	20%	20%	20%		6
Pagaduría	[E.28] indisponibilidad del personal	10	40%				6
	[A.29] Extorsión	1/10	10%	10%	10%		1
	[A.30] Ingeniería Social	1	20%	20%	20%		6
Celadores	[E.28] indisponibilidad del personal	10	40%				6
	[A.29] Extorsión	1/10	10%	10%	10%		1

Tabla 15. (Continuación)

Activos	**Amenazas**	**frecuencia**	**D**	**I**	**C**	**A**	**T**
	[A.30] Ingeniería Social	1	20%	20%	20%		6
Comité de padres	[E.28] indisponibilidad del personal	10	40%				6
	[A.29] Extorsión	1/10	10%	10%	10%		1
	[A.30] Ingeniería Social	1	20%	20%	20%		6

Fuente: el autor

11. CALCULO DEL RIESGO

Tabla 22. *Descripción de valores del riesgo.*

Riesgo		
Valor	Descripción	Valor n°
MA	Crítico	5
A	Importante	4
M	Apreciable	3
B	Bajo	2
MB	Despreciable	1

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro 3-

Tabla 23*. Valores de escala cálculo de riesgos.*

Riesgo		Probabilidad				
		MP	P	N	F	MF
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro 3-

Los riesgos que posean valores A o MA requieren atención inmediata. A continuación se presentan las tablas y los resultados obtenidos.

El riesgo es igual a la probabilidad por el impacto y esta dada en la siguiente escala :

Muy bajo = 1 a 4.
Bajo = 5 a 10
Medio = 11 a 15
Alto = 16 a 20
Muy alto = 21 a 25

Tabla 24. Calculo del riesgo

Activos	Amenazas	Probabilidad	Impacto	Riesgo
Computadores portátiles	[N.2] Daños por agua	5	5	25
	[I.8] Fallo de servicios de comunicaciones	4	4	16
	[I.5] Avería de origen físico o lógico	4	3	12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	2	2	4
	[I.10] Degradación de los soportes de almacenamiento de la información	4	3	12
	[E.14] Escapes de información.	5	5	25
	[E.23] Errores de mantenimiento, actualización de equipos hardware	4	4	16
	[E.25] Pérdida de equipos	4	4	16
	[A.22] Manipulación de programas.	5	4	20
	[A.6] Abuso de privilegios de acceso	4	5	20
	[A.7] Uso no previsto	3	4	12
	[A.23] Manipulación de los equipos.	4	4	16
Computadores de mesa	[N.2] Daños por agua	5	5	25
	[I.8] Fallo de servicios de comunicaciones	4	4	16
	[I.5] Avería de origen físico o lógico	4	3	12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	2	2	4
	[I.10] Degradación de los soportes de almacenamiento de la información	4	3	12
	[E.14] Escapes de información.	5	5	25
	[E.23] Errores de mantenimiento, actualización de equipos hardware	4	4	16

Tabla 18. (Continuación)

Activos	Amenazas	Probabilidad	Impacto	Riesgo
Computadores de mesa	[E.25] Pérdida de equipos	4	4	16
	[A.22] Manipulación de programas.	5	4	20
	[A.6] Abuso de privilegios de acceso	4	5	20
	[A.7] Uso no previsto	3	4	12
	[A.23] Manipulación de los equipos.	4	4	16
	[I.6] Suministro eléctrico	4	5	20
Sistema de Información	[E.1] Errores de los usuarios	3	4	12
	[E.8] Difusión de software dañino	5	4	20
	[E.20] Vulnerabilidades del programa (software)	4	3	12
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	5	4	20
	[A.7] Uso no previsto	3	4	12
	[A.24] Denegación de servicios	4	4	16
	[A.11] Acceso no autorizado	5	4	20
	[A.6] Abuso de privilegios de acceso	5	5	25
Antivirus	[E.8] Difusión de software dañino	5	4	20
	[E.20] Vulnerabilidades de los programas (software)	4	3	12
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	5	4	20
Sistema Operativo	[I.5] Avería de origen físico o lógico	4	3	12
	[E.1] Errores de los usuarios	4	3	12

Tabla 18. (Continuación)

Activos	Amenazas	Probabilidad	Impacto	Riesgo
	[E.8] Difusión de software dañino	4	4	16
	[E.20] Vulnerabilidades de los programas (software)	4	3	12
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	4	4	16
	[A.7] Uso no previsto	5	4	20
Aplicación web	[E.1] Errores de los usuarios	4	4	16
	[E.8] Difusión de software dañino	5	4	20
	[E.20] Vulnerabilidades del programa (software)	5	5	25
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	4	3	12
	[A.7] Uso no previsto	4	4	16
	[A.24] Denegación de servicios	5	4	20
	[A.11] Acceso no autorizado	5	5	25
	[A.6] Abuso de privilegios de acceso	5	5	25
Impresoras	[I.5] Avería de origen físico o lógico	4	3	12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	2	2	4
	[E.23] Errores de mantenimiento, actualización de equipos hardware	2	3	6
	[A.11] Acceso no autorizado	2	2	4
Router	[N.1] Fuego	2	3	6
	[N.2] Daños por agua	2	3	6

Tabla 18. (Continuación)

Activos	Amenazas	Probabilidad	Impacto	Riesgo
	[I.5] Avería de origen físico o lógico	4	3	12
	[I.7] Condiciones inadecuadas de temperaturas o humedad	2	2	4
	[A.11] Acceso no autorizado	4	3	12
	[E.4] Errores de configuración	4	4	16
Telefonía	[A.11] Acceso no autorizado	2	2	4
Red WIFI	[I.4] Fallo de servicios de comunicaciones	4	5	20
	[E.8] Errores de re-encaminamiento	4	3	12
INTERNET	[I.8] Fallo de servicios de comunicaciones	5	4	20
	[E.15] Alteración de la información	5	5	25
Documentación digital de procesos.	[A.11] Acceso no autorizado	5	5	25
	[E.15] Alteración de la información	5	4	20
	[A.15] Modificación de la información	5	5	25
	[A.25] Robo de la información	5	5	25
Documentación digital del Sistema de Información.	[A.11] Acceso no autorizado	4	4	20
	[E.15] Alteración de la información	5	4	20
	[A.15] Modificación de la información	5	4	20
	[A.25] Robo de la información	5	5	25
Informes en digital y físico	[A.11] Acceso no autorizado	4	4	16
	[E.15] Alteración de la información	5	4	20
	[A.15] Modificación de la información	5	4	2
	[A.25] Robo de la información	5	5	25

Tabla 18. (Continuación)

Activos	Amenazas	Probabilidad	Impacto	Riesgo
Antenas	[I.4] Contaminación electromecánica	2	2	4
Sede institución educativa	[N.1] Fuego	2	3	6
	[N.2] Daños por agua	2	3	2
	[.*] Desastres naturales.	2	3	6
	[A.27] Ocupación enemiga	4	2	8
Coordinador	[E.28] indisponibilidad del personal	2	3	6
	[A.29] Extorsión	1	1	1
	[A.30] Ingeniería Social	2	3	6
Docentes	[E.28] indisponibilidad del personal	2	3	6
	[A.29] Extorsión	1	1	1
	[A.30] Ingeniería Social	2	3	6
Secretaria	[E.28] indisponibilidad del personal	2	3	6
	[A.29] Extorsión	1	1	1
	[A.30] Ingeniería Social	2	3	6
Pagaduría	[E.28] indisponibilidad del personal	2	3	6
	[A.29] Extorsión	1	1	1
	[A.30] Ingeniería Social	2	3	6
Celadores	[E.28] indisponibilidad del personal	2	3	6
	[A.29] Extorsión	1	1	1
	[A.30] Ingeniería Social	2	3	6
Comité de padres	[E.28] indisponibilidad del personal	2	3	6

Tabla 18. (Continuación)

Activos	Amenazas	Probabilidad	Impacto	Riesgo
	[A.29] Extorsión	1	1	1
	[A.30] Ingeniería Social	2	3	6

Fuente: el autor.

12. ANÁLISIS DE APLICACIÓN WEB DE LA INSTITUCIÓN

Se hace un reconocimiento de los procedimientos y funciones de la aplicación web usada por docentes y secretaria.

Tabla 25. Funcionalidades de los usuarios

APLICACIÓN WEB: http://www.libretaescolar.com
Funcionalidades DE LOS USUARIOS
Funcionalidades de la secretaria: gestionar (crear, ver, actualizar y eliminar) los datos de estudiantes y profesores en el sistema, gestionar actas y menciones de honor.
Funcionalidades del docente: gestionar (crear, ver, actualizar y eliminar) los datos de logros, faltas y notas de cada periodo en las materias que tiene asignadas y el diario de cada estudiante
Funcionalidades del coordinador : consultar reportes sobre las notas y boletines de cada curso, también podrá gestionar los permisos (faltas justificadas), faltas no justificadas y permisos de los docentes
Funcionalidades del rector: para este caso el rector y el coordinador tienen asignados los mismos privilegios en la aplicación web.
Inicio de sesión de todos los usuarios que usen la aplicación

Fuente: el autor.

Login de usuarios en la aplicación web consta de: Contraseña de institución, usuario y contraseña de usuario.

Figura 4. Login de usuarios

Fuente: http://www.libretaescolar.com/index.php

Módulos especificados para cada usuario.

Tabla 26. Usuario docente

USUARIO DOCENTE	
PROCEDIMIENTOS	**DESCRIPCION**
Desempeños	El docente ingresa los desempeños de acuerdo a la escala de valores asignados los cuales serán codificados.
Planilla notas	El docente ingresa las notas de los estudiantes en cada área y especifica los códigos codificados para cada desempeño.
Observador	Se podrá llevar un registro diario de las observaciones realizadas al estudiante.

Tabla 20. (Continuación)

USUARIO DOCENTE	
PROCEDIMIENTOS	**DESCRIPCION**
Informe de periodo	En esta opción se puede generar los boletines de un periodo al que anteriormente se le han asignado desempeños y notas a cada estudiante.
Lista auxiliar	Genera en pdf el listado de estudiantes y grados asignados a un docente.
Lista de desempeños	Genera un pdf con los desempeños ingresados, clasificados por área y con su respectivo código
Resumen notas	Genera un pdf con el listado de estudiantes y las notas definitivas en cada área y también especifica el puesto ocupado por cada estudiante según su rendimiento académico
Estadística de periodo	Genera una estadística grafica del rendimiento académico de todos los grados, según sus calificaciones.

Fuente: el autor

Tabla 27. Usuario secretaria

USUARIO SECRETARIA	
PROCEDIMIENTOS	**DESCRIPCION**
Desempeños	Puede visualizar los desempeños y adicionar.
Docente	Se tiene la información de los docentes y se le puede cambiar el tipo de usuario en caso de ser necesario, también lo puede desactivar para quitar los privilegios asignados.

Tabla 21. (Continuación)

USUARIO SECRETARIA	
PROCEDIMIENTOS	**DESCRIPCION**
Generar planillas	Genera las planillas de todos los grados para cada periodo lectivo.
Informe de periodo	En esta opción se puede generar los boletines de un periodo al que anteriormente se le han asignado desempeños y notas a cada estudiante.
Lista auxiliar	Genera en pdf el listado de estudiantes y grados asignados a un docente.
Planilla notas	Están los listados de cada grado y de cada área con las notas asignadas por los docentes y estas pueden ser modificadas en caso de errores solo por la secretaria.
Resumen faltas	Genera un pdf con el listado de estudiantes con las faltas de cada periodo.
Resumen notas	Genera un pdf con el listado de estudiantes y las notas definitivas en cada área y también especifica el puesto ocupado por cada estudiante según su rendimiento académico
Estadística de periodo	Genera una estadística grafica del rendimiento académico de todos los grados, según sus calificaciones.

Fuente: el autor

Tabla 28. Usuario coordinador y rector

USUARIO COORDINADOR Y RECTOR	
PROCEDIMIENTOS	**DESCRIPCION**
Desempeños	Puede visualizar los desempeños y adicionar.
Docente	Se tiene la información de los docentes y se le puede cambiar el tipo de usuario en caso de ser necesario, también lo puede desactivar para quitar los privilegios asignados.
Generar planillas	Genera las planillas de todos los grados para cada periodo lectivo.
Informe de periodo	En esta opción se puede generar los boletines de un periodo al que anteriormente se le han asignado desempeños y notas a cada estudiante.
Adicionar usuario	Puede crear un usuario nuevo asignando el tipo de usuario.
Plazo notas	Puede habilitar la aplicación para que pueda ser usada por los docentes, asignando una fecha de apertura y cierre de cada periodo para el ingreso de desempeños y notas.
Periodos	Adiciona los periodos que tiene el año lectivo y asigna un porcentaje a cada periodo en donde la suma de estos debe ser el 100% que corresponde al informe final.

Tabla 22. (Continuación)

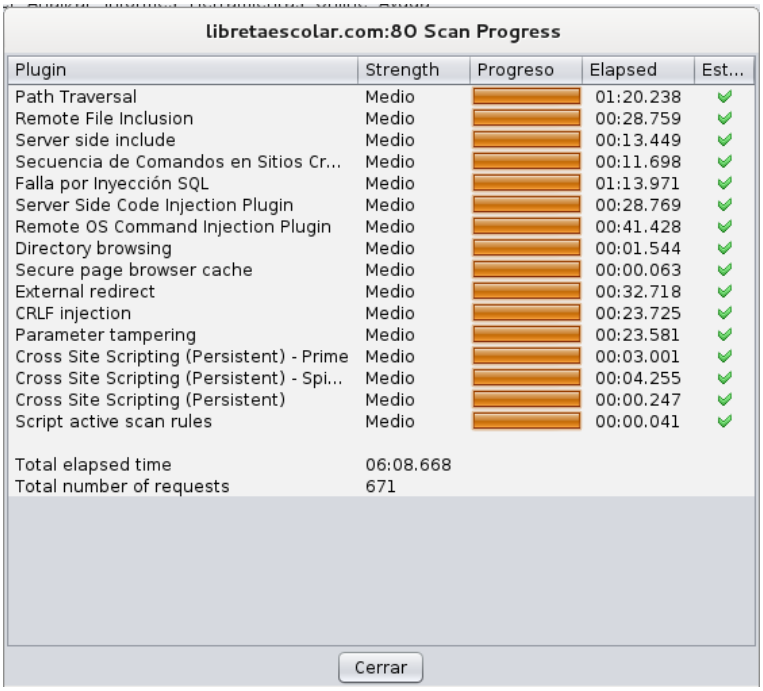
USUARIO COORDINADOR Y RECTOR	
PROCEDIMIENTOS	**DESCRIPCION**
Resumen faltas	Genera un pdf con el listado de estudiantes con las faltas de cada periodo.
Resumen notas	Genera un pdf con el listado de estudiantes y las notas definitivas en cada área y también especifica el puesto ocupado por cada estudiante según su rendimiento académico
Estadística de periodo	Genera una estadística grafica del rendimiento académico de todos los grados, según sus calificaciones.

Fuente: el autor

12.1. ESCANEO DE VULNERABILIDADES DE APLICACIÓN WEB

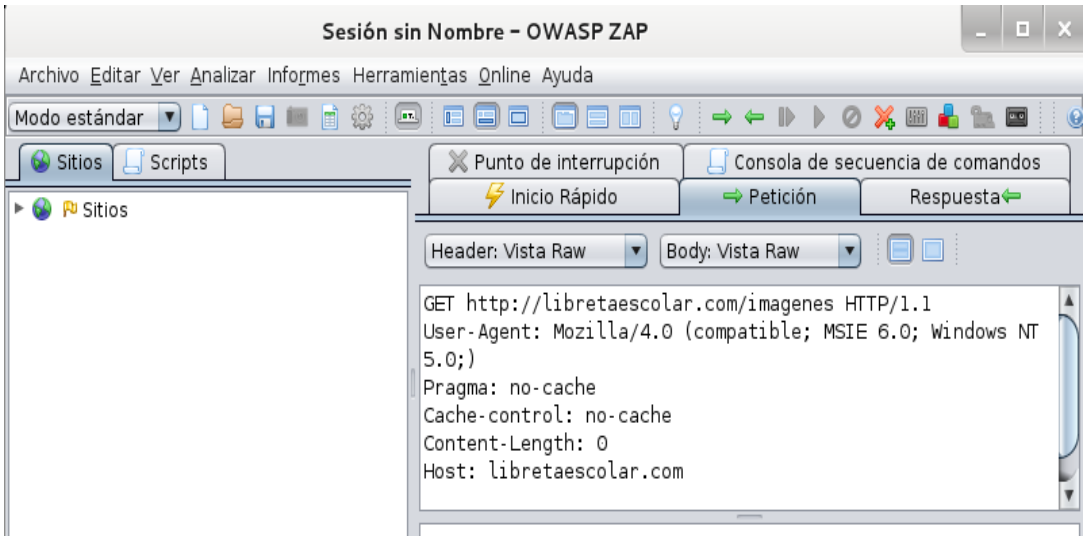
Para el escaneo de vulnerabilidades de la aplicación web usada por la Institución Educativa se usa la herramienta OWASP ZAP que es idónea para verificar la seguridad de la aplicación web en el presente análisis

Figura 5. Herramienta OWASP ZAP



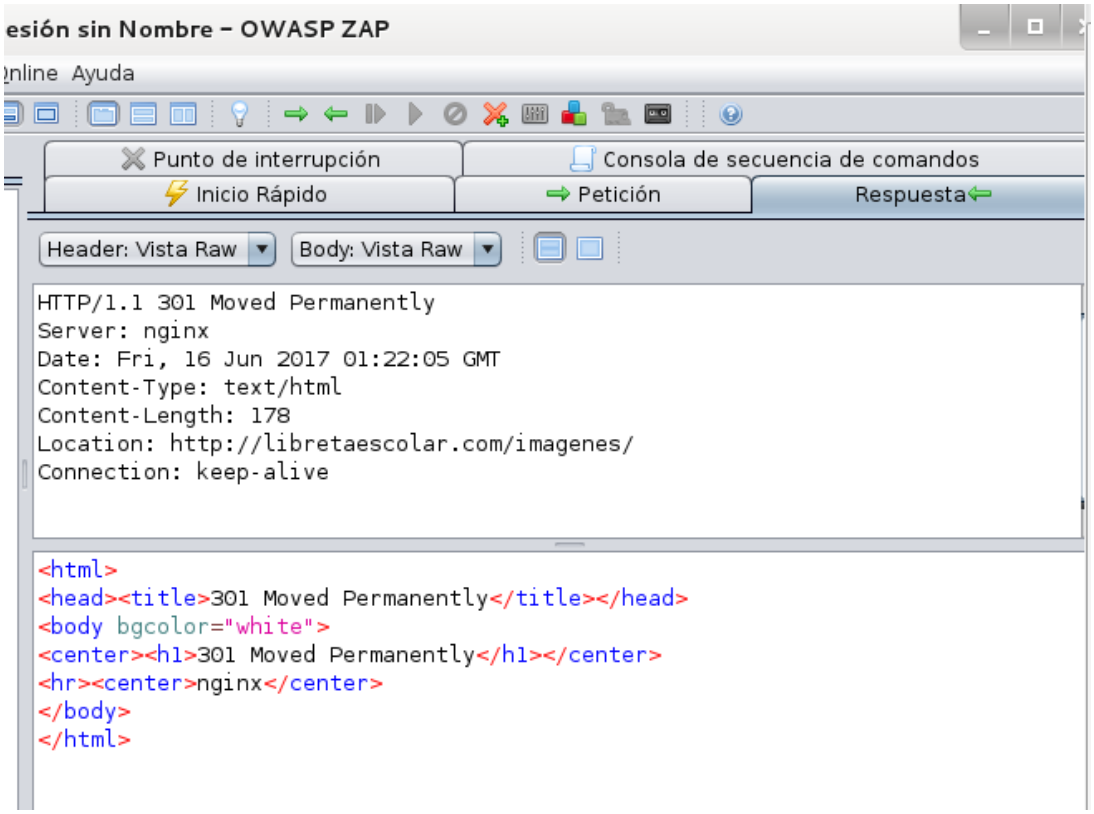
Fuente: El autor

Figura 6. Petición herramienta OWASP ZAP



Fuente: El autor

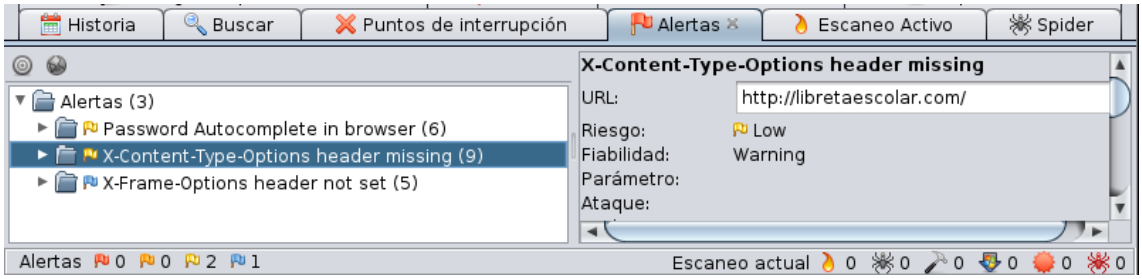
Figura 7. Respuesta herramienta OWASP ZAP



Fuente: El autor

En el escaneo de vulnerabilidades con la herramienta owasp –zap en el sistema operativo kali Linux de la aplicación www.libretaescolar.com se detectaron las tres vulnerabilidades que se muestran a continuación:

Figura 8. Vulnerabilidades encontradas con la herramienta OWASP ZAP.



Fuente: El autor

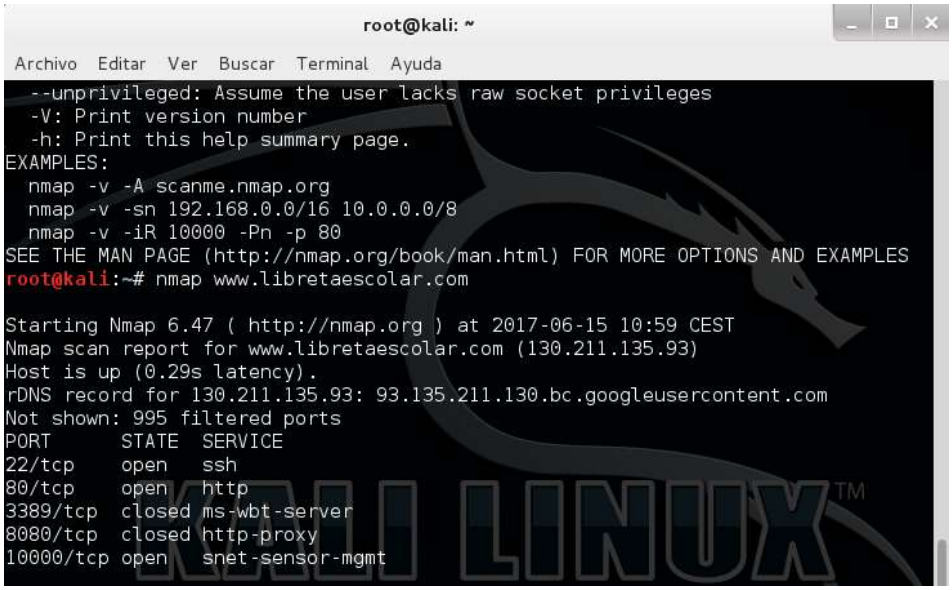
Vulnerabilidad x -contens –type-options header missing : Este error que presenta la aplicación analizada permite que antiguas versiones de internet Explorer y google Chrome ejecuten NIME-sniffing en el cuerpo de la respuesta, ocasionando que esta se interprete y se muestre como un tipo de contenido no declarado. Las versiones actuales y oficiales de Firefox utilizan tipos de contenido declarado, en lugar de realizar MIME-sniffing

Vulnerabilidad x frame- options header not set (5): El encabezado X-Frame-Options no está incluido en la respuesta HTTP para proteger contra ataques 'ClickJacking'.

Vulnerabilidad password : El atributo AUTOCOMPLETE no está deshabilitado en el elemento HTML FORM / INPUT que contiene la entrada de tipo de contraseña. Las contraseñas se pueden almacenar en los navegadores y recuperarse.

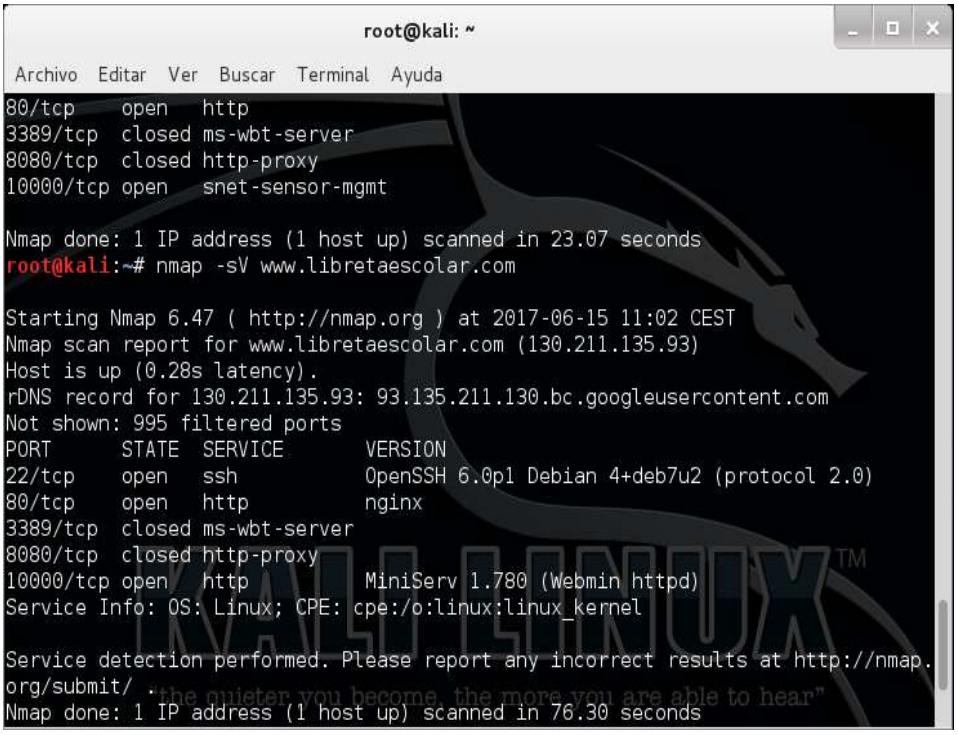
Herramienta Nmap del sistema operativo Kali Linux usada para la identificación de las siguientes características de la aplicación web.

Figura 9 Herramienta nmap Servicios



Fuente: El autor

Figura 10. Herramienta nmap Sondeo de puertos tcp reservados en el servidor

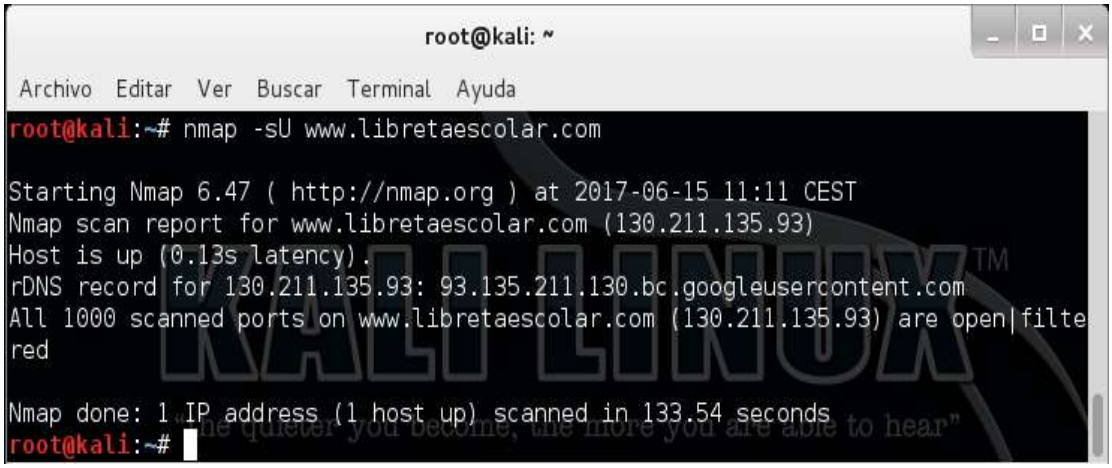


Fuente: El autor

figura 11. Identificación de host activos en la red

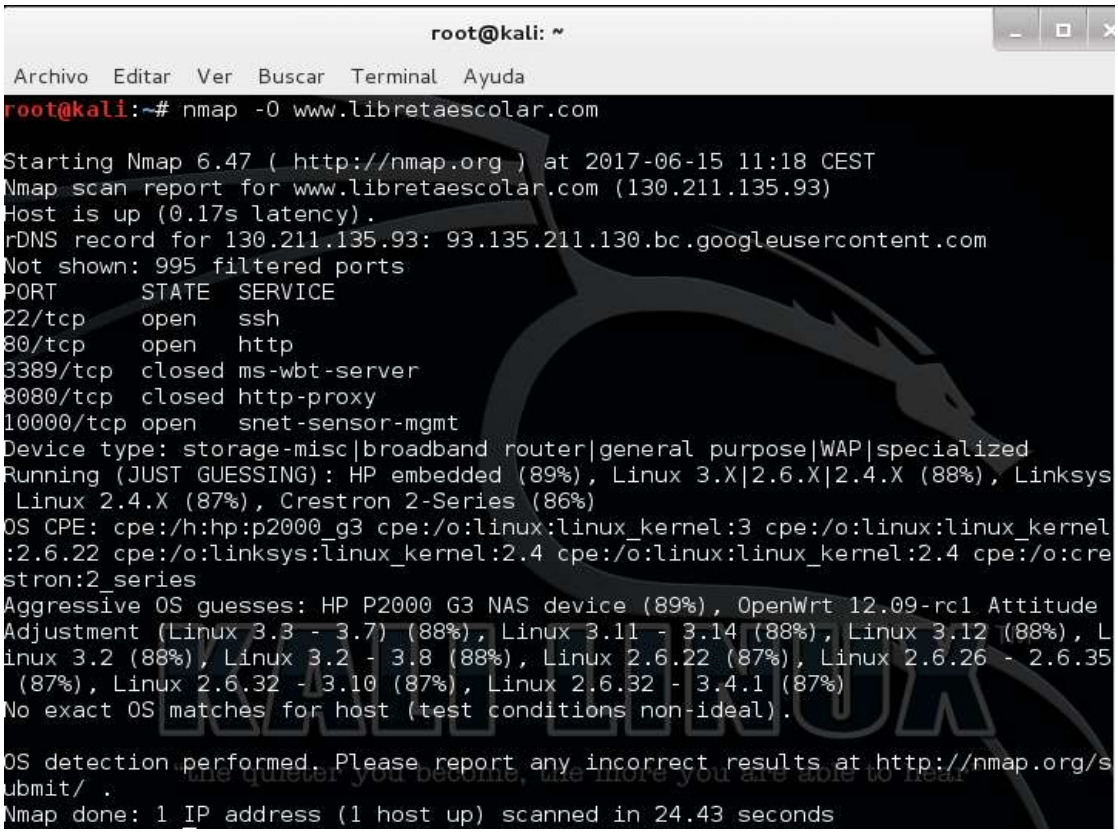
Fuente: El autor

figura 12. Barrido de puertos por udp



Fuente: El autor

Figura 13. Sistema operativo usado



Fuente: El autor

Dentro del reconocimiento de los diferentes procedimientos que se realizan en la aplicación web de acuerdo al rol asignado a cada usuario se logró identificar los siguientes aspectos que comprometen la integridad, la disponibilidad y confiabilidad de los datos que se manejan en la aplicación web y que afectan directamente el desarrollo del procedo gestión académica de la Institución:

En el rol de los docentes esta la opción de generar un borrador de los informes finales de cada estudiante, este es generado en un pdf con una marca de agua con la palabra borrador, este archivo no cuenta con las condiciones mínimas de seguridad ya que se permite cambiar al formato del procesador de texto de Microsoft Word sin ninguna dificultad, el archivo en pdf no está cifrado y se presta para la manipulación y modificación de la información presente en el informe de periodo de cada estudiante, este es un documento vital para los procedimientos académicos de los estudiantes.

Dentro del plan de respaldo de copias de seguridad de la aplicación web, se identificó que están programados para realizarse semanalmente , pero debido a que la aplicación es usada solo en las fechas establecidas para los cuatro periodos académicos con los que cuenta la institución, y en dichas fechas se usa la aplicación a diario y se realizan diferentes procedimientos, durante estas fechas no se realizan copias de seguridad diaria, y de acuerdo a la información suministrada por la secretaria la aplicación generó un error después de haber impreso los informes finales y varias calificaciones aparecieron en blanco al siguiente día, la información no se logró recuperar porque no había copia de seguridad actualizada y la única solución fue corregirlo nuevamente de forma manual en la aplicación web. Esta situación genera un margen alto en la seguridad de la información especialmente en su disponibilidad lo que ocasiona retrasos en los procedimientos.

Las políticas de acceso para la aplicación web no han sido socializadas con los usuarios, dicho desconocimiento pone en juego la confidencialidad, la disponibilidad y la integridad de los datos.

Cada año se realiza el cambio de usuarios y contraseñas para el ingreso a la aplicación web a los usuarios, la caducidad de las contraseñas no son las indicadas, debido a que se recomienda que estas sean modificadas cada tres meses, además se identificó que las contraseñas asignadas no son robustas, ya que contienen menos de seis caracteres y se puede descifrar de forma fácil, el proceso de login de usuario carece de autentificación porque la aplicación no cuenta con el bloqueo temporal al usuario por el ingreso de cierto número de intentos fallidos, al digitar la contraseña incorrecta y no realiza el informe correspondiente de dicho proceso al administrador para que pueda evitar la posible suplantación de usuario.

13. IDENTIFICACIÓN Y SELECCIÓN DE CONTROLES ISO/IEC 27001:2013

La normatividad internacional ayuda a establecer que controles se deben aplicar para los activos de información, siendo estas guías de buenas prácticas, la ISO/IEC 27001:2013, contiene 114 controles, agrupados en 14 dominios, el documento primordial llamado declaración de aplicabilidad nace de identificar cuáles de los 114 controles aplican en la organización. La siguiente tabla muestra la identificación de los controles requeridos según la identificación, valoración y evaluación de los riesgos y amenazas del sistema informático para los cuales se realiza una justificación de su elección para la institución.

Tabla 29. Matriz de declaración de aplicabilidad (SOA)

LR : requisitos legales
CO: obligaciones contractuales
BR / BP : los requerimientos del negocio / mejores prácticas adoptadas
RRA : resultados de la evaluación de riesgos , TSE: hasta cierto punto

ISO/IEC 27001:2013 Anexo A controles			**Aplica**	**justificación de las exclusiones**	**controles seleccionados**				**justificación de la elección del control**
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/ BP**	**RRA**	
	5.1	**Directrices de la administración para las políticas de seguridad de la información**							
5. Políticas de seguridad	5.1.1	Políticas de seguridad de la información	X				x	x	La Institución no cuenta con políticas de seguridad de la información. Es necesario crear las políticas de seguridad de la información de la institución de acuerdo a sus necesidades y objetivos principales y posteriormente socializadas a todos sus integrantes para resaltar la importancia de las políticas de seguridad de la información planteadas y su cumplimiento.

Tabla 23.(Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	5.1.2	Revisión de las políticas de seguridad de la información	x				x	x	Las políticas se deben revisar como mínimo una vez al año con el fin de implementar mejoras de acuerdo a los requerimientos de la institución y sus cambios deben ser socializados.
	6.1	**Organización Interna**							
6 Organización de la seguridad de la información	6.1.1	Roles y responsabilidades para la seguridad de la información	x				x		
	6.1.2	Separación de deberes	x				x		

Tabla 23.(Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	6.1.3	Contacto con las autoridades	X		x		x		
	6.1.4	Contacto con grupos de interés especial	X		x		x		
	6.1.5	Seguridad de la información en la gestión de proyectos	X				x		
	6.2	**Dispositivos móviles y teletrabajo**							
	6.2.1	Política para dispositivos móviles	X				x		

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	6.2.2	Teletrabajo	no	El teletrabajo de acuerdo a la normativa de la ley 1221 de 2008, permite a los trabajadores la prestación de sus servicios sin la presencia física en su sitio de trabajo, realizando sus actividades laborales a través de las tecnologías de la información y la comunicación (TIC), lo cual no aplicaría para la institución educativa ya que sus trabajadores atienden a una comunidad infantil y requiere la presencia por parte de sus trabajadores.					

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	7.1 Antes de asumir el empleo								
7. Seguridad de los recursos humanos	7.1.1	Selección	No	La institución educativa por ser una entidad pública no realiza ningún proceso de selección de sus empleados ya que ellos son asignados directamente por la secretaria de educación.					
	7.1.2	Términos y condiciones del empleo	no	Los términos y condiciones del empleo son realizados por secretaria de educación municipal por medio de un acto administrativo.					

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	7.1.1	Selección	No	La institución educativa por ser una entidad pública no realiza ningún proceso de selección de sus empleados ya que ellos son asignados directamente por la secretaria de educación municipal, mediante un acta de nombramiento fija o con provisionalidad.					
	7.1.2	Términos y condiciones del empleo	no	Los términos y condiciones del empleo son realizados por secretaria de educación municipal por medio de un acto administrativo.					

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	7. 2 Durante la ejecución del empleo								
	7.2.1	Responsabilidades de la dirección	x			x	x	x	La dirección de la institución se debe encargar de la creación, socialización e implementación de las políticas de seguridad de la información y que están vayan complementadas con el objetivo principal de la institución.
	7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	x				x	x	todos los empleados de la institución deben conocer las políticas de seguridad de la información a través de capacitaciones que sensibilicen sobre la importancia de dichas políticas, los riesgos que se corren, sus deberes de acuerdo a las funciones establecidas y responsabilidades correspondientes a la seguridad de la información

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Clausula	**Sección**	**Control**			**LR**	**CO**	**BR/BP**	**RRA**	
	7.2.3	Procesos disciplinario	x			x	x	x	La institución debe establecer un proceso disciplinario cuando los empleados cometan una falta en la seguridad de la información, llevando a cabo un registro de incumplimiento de las políticas de seguridad de información establecidas y su debido seguimiento.
	7.3 Terminación y cambio de empleo								
	7.3.1	Terminación o cambio de responsabilidades de empleo	x			x	x	x	Se debe implementar un proceso documentado en donde se especifique la terminación o cambio de responsabilidades de los empleados, teniendo en cuenta el retiro de derechos de acceso, verificación y entrega de activos a cargo del empleado en caso de

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	7.3.1	Terminación o cambio de responsabilidades de empleo	x			x	x	x	Retiro, la entrega del documento y su socialización en caso de cambio de responsabilidades de acuerdo a lo establecido en las políticas de seguridad de la información.
	8.1 Responsabilidad por los activos								
8. Gestión de activos	8.1.1	Inventario de activos	X				x	x	La institución debe realizar un inventario de activos de información y clasificado de acuerdo al área a la que corresponde y este debe ser actualizado constantemente.
	8.1.2	Propiedad de los activos	x				x	x	Se necesita realizar actas a las personas que manejan los activos de la institución y que están bajo su cargo, que contengan las recomendaciones necesarias para la seguridad de la información de dichos activos.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	8.1.3	Uso aceptable de los activos	x				x	x	Se debe realizar manual de manejo adecuado de los activos según su clasificación y basado en las políticas de la seguridad de la información.
	8.1.4	Devolución de activos	x				x	x	Se debe crear un formato para la entrega de activos que están dañados para que sean dados de baja.
	8.2 Clasificación de información								
	8.2.1	Clasificación de la información	x				x	x	La información en la institución se debe clasificar, en primera instancia teniendo en cuenta la ley de protección de datos personales, datos sensibles y datos personales, el valor que tienen para la institución, su grado criticidad y la modificación no autorizada

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	8.2.2	Etiquetado de la información	x				x	x	Se debe establecer un procedimiento para etiquetar la información de acuerdo a la clasificación definida
	8.2.3	Manejo de activos	x				x	x	Se necesita establecer procedimiento de manejo de los activos de acuerdo a la seguridad de la información, con referencia al procesamiento, almacenamiento y comunicación de la información de la institución.
	8.3 Manejo de medios								
	8.3.1	Gestión de los medios removibles	x				x	x	La institución usa diferentes medios extraíbles para la transferencia de datos sensibles de información, a sus empleados por medio de usb,CD y correo electrónico, por esta razón es necesario que se establezcan controles de seguridad que permitan proteger la

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	8.3.1	Gestión de los medios removibles	x				x	x	Información y que no se vea afectada la integridad y la confidencialidad de los datos y en algunos casos usar las técnicas de la criptografía para los datos más sensibles.
	8.3.2	Disposición de los medios	x	.			x	x	Se deben formalizar los procedimientos para el almacenamiento y eliminación segura de los medios protegiendo la información sensible que tienen dichos medios.
	8.3.3	Transferencia de medios físicos	x				x	x	Los empleados de la institución usan medios físicos con información y para ello se debe establecer los controles necesarios para que sean protegidos contra accesos no autorizados

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	9.1 Requisitos del negocio para el control de acceso								
9.Control de acceso	9.1.1	Política de control de acceso	x				x	x	Se debe definir la policita de control de acceso: Solo personal autorizado puede acceder a los activos de información identificados y etiquetados según la clasificación realizada, todo acceso debe ser registrado, documentado y verificado. Se deben aplicar mecanismos para controlar el acceso a nivel de sistema operativo, acceso a la red, acceso físico y acceso lógico.
	9.1.2	Acceso a redes y a servicios de red	x				x	x	La institución debe realizar una política para el uso de redes y servicios de red con el fin de minimizar los riesgos como el acceso no autorizado, malware o manipulación de la información.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	9.2	**Gestión del acceso de usuarios**							
	9.2.1	Registro y cancelación del registro de usuarios	x				x	x	La institución debe establecer un ID para cada usuarios dando a conocer las responsabilidades y el manejo de la ID para hacer un buen uso de la red, sus servicios y la aplicación web con la que cuenta la institución. De igual forma se debe establecer los procedimientos de cancelación de usuarios que se retiran. Se debe eliminar las cuentas de usuario de la aplicación web que no cumplen con la política de control de acceso.
	9.2.2	Suministro de acceso a usuarios	x				x	x	Se debe realizar un procedimiento para la asignación de acceso al usuario en donde se pueda identificar el registro y la cancelación de los usuarios,

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones				controles seleccionados				justificación de la elección del control
				LR	CO	BR/BP	RRA					
	9.2.2	Suministro de acceso a usuarios	x							x	x	Además es indispensable capacitar y concientizar a los usuarios sobre este procedimiento.
	9.2.3	Gestión de derechos de acceso privilegiado	x									De acuerdo a la asignación de roles y su clasificación de las áreas correspondientes, se debe asignar control de acceso y los privilegios especiales de cada rol identificado para los usuarios de la institución.
	9.2.4	Gestión de información de autenticación secreta de usuarios	x							x	x	La institución debe en primera instancia identificar los servicios que necesitan el uso de una contraseña cifrada y posteriormente realizar una gestión que permita el control de la asignación de información de autenticación.
	9.2.5	Revisión de los derechos de acceso de usuarios	x							x	x	La institución debe hacer una revisión de derechos de acceso en forma regular con el fin de verificar si los

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones				controles seleccionados				justificación de la elección del control
				LR	CO	BR/BP	RRA					
	9.2.5	Revisión de los derechos de acceso de usuarios	x							x	x	Usuarios poseen los derechos de acceso pertinentes.
	9.2.6	Retiro o ajuste de los derechos de acceso	x							x	x	Se debe realizar un procedimiento de retiro de los derechos de acceso físico y lógico a las personas que sean desvinculadas de la institución o con traslado, de acuerdo a las políticas de acceso establecidas por la institución.
	9.3	**Responsabilidades de los Usuarios**										
	9.3.1	Uso de información de autenticación secreta	x							x	x	Los usuarios deben seguir las prácticas de la institución en el uso de información secreta de autenticación, planteadas dentro de las políticas de seguridad de la información

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
					LR	CO	BR/BP	RRA	
	9.4	**Control de acceso a sistemas y aplicaciones**							
	9.4.1	Restricción del acceso a la información	x		x		x	x	Se debe documentar y formalizar que solo el personal autorizado puede acceder a los activos de información identificados y etiquetados según la clasificación realizada, todo acceso debe ser registrado, documentado y verificado. Se deben aplicar mecanismos para controlar el acceso a nivel de sistema operativo, acceso a la red, acceso físico y acceso lógico.
	9.4.2	Procedimiento de ingreso seguro	x				x	x	La institución debe implementar un inicio de sección seguro para los servicios y las aplicaciones con las que cuenta.
	9.4.3	Sistema de gestión de contraseñas	x				x	X	La institución necesita la implementación de un sistema de gestión de

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones				controles seleccionados				justificación de la elección del control
				LR	CO	BR/BP	RRA					
	9.4.3	Sistema de gestión de contraseñas	x							x	x	Contraseñas que sean interactivas y de calidad, además debe contener un software capaz de proteger las a través de algoritmos criptográficos fuertes.
	9.4.4	Uso de programas utilitarios privilegiados	x							x	x	La institución debe establecer parámetros referentes al uso de programas utilitarios que puedan comprometer la seguridad de la información y se debe asignar privilegios de estos programas solo al personal idóneo, de igual manera se debe impedir la instalación de algún programa o software no autorizado.
	9.4.5	Control de acceso al código fuente de los programas	x							x	x	La institución debe establecer restricciones en el acceso al código fuente de la aplicación, para su protección y evitar riegos como la implementación de

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
					LR	CO	BR/BP	RRA	
	9.4.5	Control de acceso al código fuente de los programas	x				x	x	Funciones no autorizadas que pueden alterar la información y su confidencialidad e integridad.
10 Criptografía	**10.1**	**Controles Criptográficos**							
	10.1.1	Política sobre el uso de controles criptográficos	x				x	x	La institución debe centrar su objetivo en la protección de la autenticidad, la integridad y la confidencialidad de la información, para ello debe implementar las políticas necesarias de cifrado de contraseñas, llaves criptográficas, verificando que toda la información enviada y recibida este cifrada.
	10.1.2	Gestión de llaves	x				x	x	La institución al no tener ningún mecanismo criptográfico que debe ser implementado, también debe crear una política de.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	10.1.2	Gestión de llaves	x				x	x	uso, protección y duración de las claves de cifrado en su ciclo de vida
11. Seguridad física y del entorno	**11.1**	**Áreas seguras**							
	11.1.1	Perímetro de seguridad física	x						La institución debe identificar las zonas de la institución en donde se encuentra la información para poder determinar los perímetros de seguridad física.
	11.1.2	Controles de acceso físicos	x				x	x	Las diferentes áreas deben ser protegidas por los controles de entrada adecuados para garantizar que se permite el acceso sólo el personal autorizado.
	11.1.3	Seguridad de oficinas, recintos e instalaciones	x						Se debe crear y aplicar una política de seguridad física y darlas a conocer a todos los usuarios para que se pueda dar su debido cumplimiento.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	11.1.4	Protección contra amenazas externas y ambientales	x				x	x	La institución debe implementar políticas de protección física contra los desastres naturales, ataques maliciosos o accidentes, esta debe ser diseñada y aplicada.
	11.1.5	Trabajo en áreas seguras							
	11.1.6	Áreas de carga, despacho y acceso público	No	La institución no cuenta con despacho de información por fuera de la sede.					
	11.2	**Equipos**							
	11.2.1	Ubicación y protección de los equipos	x				x	x	La institución posee una variedad de equipos en donde se procesa y se almacena la información de los diferentes procedimientos realizados, debido a ello es necesario que se establezcan controles sobre la ubicación

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	11.2.1	Ubicación y protección de los equipos	x				x	x	Y protección contra los diferentes riesgos de accesos no autorizados o riesgos ambientales, que puedan generar algún daño, interrupción o robo de los equipos de la institución perjudicando directamente los activos de la información.
	11.2.2	Servicios de suministro	x				x	x	La institución no cuenta con una protección para las fallas de suministro de energía lo que puede provocar una interrupción en los procedimientos realizados
	11.2.3	Seguridad del cableado	x				x	x	La institución debe establecer parámetros para la seguridad del cableado ya que este transporta datos que pueden ser interceptados por este medio, el cableado de la institución debe ser certificado.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	11.2.4	Mantenimiento de los equipos	x				x	x	Realizar la verificación del programa de mantenimiento de equipos de acuerdo a sus especificaciones y las fichas de los procesos realizados a cada equipo.
	11.2.5	Retiro de activos	x				x	x	Se debe hacer la salida respectiva mediante un documento formal a los elementos que han sido dados de baja, para evitar su acumulación.
	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	no	La institución educativa por ser de carácter público establece que sus equipos y activos no pueden salir de las instalaciones					
	11.2.7	Disposición segura o reutilización de equipos	x				x	x	Se debe realizar un procedimiento para la reutilización de los equipos verificando la información almacenada en ellos y proceder a la eliminación

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									Segura para que el equipo pueda ser reutilizado.
	11.2.8	Equipo de usuario desatendido	x				x	x	Se deben implementar controles para los equipos desatendidos que permitan protegerse mediante mecanismos de bloqueo con contraseña, la protección de las terminales
	11.2.9	Política de escritorio despejado y de pantalla despejada	x						La institución carece de la política de escritorio despejado y pantalla despejada por ello debe creada y socializada a sus usuarios con la sensibilización respectiva.
	12.1	**Procedimientos Operacionales y Responsabilidades**							
12.Seguridad de las operaciones	12.1.1	Procedimientos de operación documentados	x				x	x	La institución debe implementar un sistema de gestión de calidad que permita documentar todos los procedimientos realizados como el procesamiento y

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									comunicación de la información en los equipos y en la aplicación web, manejo de correo, inicio y cierre de sección de los equipos, que deben estar listo para los usuarios que los requieran.
	12.1.2	Gestión de cambios	x	.			x	x	Las políticas de gestión de cambios se debe establecer en la institución ya que esta le permite identificar y controlar los cambios realizados a nivel de procesos de la institución o las instalaciones del procesamiento de la información, esta gestión permite identificar, evaluar el cambio, probarlo y comunicarlo a sus empleados de manera oportuna.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	12.1.3	Gestión de la capacidad	x				x	x	De acuerdo a las proyecciones de la institución para su crecimiento se debe verificar la capacidad de procesamiento de los sistemas y su eficiencia que den cumplimiento a lo proyectado por la institución para todos sus procedimientos.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación							
	12.2	**Protección contra código malicioso**							
	12.2.1	Controles contra código malicioso	x				x	x	La institución debe crear controles contra el código malicioso, como la restricción de software no autorizado, uso de sitios web desconocidos, vulnerabilidades técnicas,

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									Revisión, instalación y actualización de software de forma periódica, realización de planes de continuidad para los ataques malware.
	12.3	**Copias de respaldo**							
	12.3.1	Copias de respaldo de la información	x				x	x	Se deben realizar copias de respaldo de la información regularmente mediante proceso de backup y recuperación que permitan proteger los datos y que se puedan restaurar de forma rápida para que no se interrumpa ningún procedimiento por falta de disponibilidad de la información.
	12.4	**Registro y monitoreo**							

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	12.4.1	Registro de eventos	x				x	x	Los usuarios de acuerdo a sus roles y responsabilidades asignadas realizan determinadas actividades y tienen accesos y privilegios a la información, debido a ello se debe establecer un registro de eventos que evidencie las actividades realizadas por los usuarios y el uso correcto de la información para que no se ponga en riesgo su seguridad.
	12.4.2	Protección de la información de registro							La integridad de los registros es importante para la institución, especialmente cuando se presentan fallos en el sistema o incidentes de seguridad y para ello es necesario tener un proceso de protección de la información de registro

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	12.4.3	Registros de actividades del administrador y del operador	x				x	x	Se deben realizar revisiones periódicas a los registros para verificar las acciones realizadas por el administrador del sistema y estos registros se deben proteger de forma adecuada
	12.4.4	Sincronización de relojes	x				x	x	La institución por pertenecer al sector público debe cumplir la normativa de que todos los equipos deben estar sincronizados con la hora legal Colombiana, por esta razón los equipos de la institución deben estar sincronizados con el protocolo NTP
	12.5	**Control de software operacional**							
	12.5.1	Instalación de software en sistemas operacionales	x				x	x	Todos los empleados de la empresa deben conocer las políticas sobre la instalación de software y sus restricciones para controlar la correcta operación de los sistemas operativos.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	12.6	**Gestión de vulnerabilidades técnicas**							
	12.6.1	Gestión de las vulnerabilidades técnicas	x						La institución debe realizar una gestión de las vulnerabilidades técnicas ya que están pueden afectar de forma considerable el sistema para ello se debe tener un inventario de activos completo y actualizado.
	12.6.2	Restricción sobre la instalación de software	x						Todos los empleados de la empresa deben conocer las políticas sobre la instalación de software y sus restricciones de acuerdo a lo estipulado por la institución.
	12,7	Consideraciones sobre auditoria de sistemas de información							

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	12.7.1	Controles de auditorías de sistemas de información	x						La institución debe establecer los controles de los sistemas de información, cuando estos hagan parte de los procesos de auditoria de la seguridad de la información, teniendo en cuenta los controles de acceso, las pruebas y su alcance y el registro de todo lo que se realice durante el proceso de auditoría.
13. seguridad de las comunicaciones	**13.1**	**Gestión de la seguridad de las redes**							
	13.1.1	Controles de las redes	x				x	x	La institución debe implementar políticas de seguridad de las redes de comunicación, que permita proteger a la información en la red y prevenir los riesgos, para ello es necesario limitar algunos servicios, realizar segmentaciones de acuerdo

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									Al nivel de criticidad de los activos, el control de acceso a los puertos, entre otros.
	13.1.2	Seguridad de los servicios de red	x				x	x	La institución debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red y estos deben ser incluidos en los acuerdos de servicios de red.
	13.1.3	Separación de las redes	x				x	x	Es indispensable que la institución separe en redes los grupos de los sistemas de información, los usuarios y los servicios de información que posee.
	13.2	**Transferencia de información**							
	13.2.1	Políticas y procedimientos para el intercambio de información	x				x	x	La institución debe implementar políticas que permitan transferir información sin poner en riesgo la confidencialidad de la información.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	13.2.2	Acuerdos sobre transferencia de información	x				x	x	La institución intercambia información con sus sedes y es necesario Establecer cláusulas de confidencialidad para la transferencia de información altamente clasificada, con el fin de garantizar la seguridad de la información enviada.
	13.2.3	Mensajería electrónica	x						Establecer políticas para el envío de correos en donde la información relevante para la institución esté debidamente cifrada.
	13.2.4	Acuerdos de confidencialidad o de no divulgación	x						La institución debe establecer acuerdo de confidencialidad y de no divulgación de la información y dichos acuerdos deben ser revisados periódicamente.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
14 Adquisición, desarrollo y mantenimiento de sistemas de información	**14.1**	**Requisitos de seguridad de los sistemas de información**							
	14.1.1	Análisis y especificación de los requisitos de seguridad de la información	x				x	x	La institución como primera medida debe tener en cuenta que los requisitos y controles de seguridad de la información identificados deben ir alineados con su misión, también debe establecer cuáles son los procesos para poder así realizar una gestión de los requisitos de la seguridad de la información y estos deben ser incluidos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
	14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	x						Es necesario crear políticas de seguridad para la seguridad de la aplicación web que maneja la institución, con el fin de proteger la información que pasa a través de redes públicas.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	14.1.3	Protección de transacciones de los servicios de las aplicaciones	x				x	x	Se deben tener controles de seguridad para las transacciones realizadas en la aplicación web que permitan proteger la información implicada en dichas transacciones evitando la falla en sus diferentes procesos que generen duplicación, divulgación o transmisión incompleta.
	14.2	**Seguridad en los Procesos de Desarrollo y Soporte**							
	14.2.1	Política de desarrollo seguro	x				x	x	Se deben documentar y evidenciar todos los procesos o cambios que se realicen al sistema de información de la institución, su objetivo es que se verifique que cumple con las características de seguridad necesarias.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	14.2.2	Procedimientos de control de cambios en sistemas	x				x	x	Se deben documentar y evidenciar todos los procesos o cambios que se realicen al sistema de la institución verificando que estos no comprometan la seguridad de la información o el desarrollo normal de las diferentes actividades realizadas.
	14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	x				x	x	Es adecuado que la institución haga un revisión técnica después de haber realizado algunas modificación en la plataforma operacional, dicha revisión técnica debe contener las pruebas necesarias para saber si la información no queda en riesgo y que no hayan impactos negativos que impidan las operaciones o que las afecten parcialmente.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	Control				LR	CO	BR/BP	RRA	
	14.2.4	Restricciones en los cambios a los paquetes de software	x				x	x	Se debe realizar un control estricto y establecer límites para los modificaciones de los paquetes software, realizando pruebas que verifiquen que la seguridad de la información no queda en riesgo, para ello estos cambios deben ser probados y documentados
	14.2.5	Principios de construcción de los sistemas seguros	x				x	x	La institución debe tener en cuenta los principios de ingeniería de seguridad de las actividades realizadas, implementando un diseño de seguridad basado en las aplicaciones, la tecnología y los datos, este diseño debe ser revisado periódicamente.
	14.2.6	Ambiente de desarrollo seguro	x						Para el desarrollo e integración de los sistemas usados en la institución se necesita establecer ambientes adecuados que

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									brinden los niveles de seguridad necesarios.
	14.2.7	Desarrollo contratado externamente	x				x	x	La institución de realizar un seguimiento adecuado de los procesos realizados por parte de los sistemas contratados externamente.
	14.2.8	Pruebas de seguridad de sistemas	x				x	x	Se necesita que la institución, basada en uno de sus objetivos principales como es la seguridad de la información establezca las pruebas necesarias que permitan verificar que los sistemas desarrollados cumplen con los requisitos de seguridad.
	14.2.9	Prueba de aceptación del sistema	x				x	x	Se deben establecer programas de pruebas para los sistemas y criterios de aceptación para los sistemas nuevos implementos o su actualización.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	14.3	**Datos de prueba**							
	14.3.1	Protección de los datos de prueba del sistema					x	x	Los datos usados en la realización de prueba deben ser protegidos y en cuanto sea posible se debe evitar usar información confidencial o que contenga información personal.
15 Relaciones con los proveedores.	**15.1**	**Seguridad de la información en las relaciones con los proveedores**							
	15.1.1	Política de seguridad de la información para las relaciones con proveedores					x	x	La institución debe establecer las políticas de seguridad de la información para el proveedor de la aplicación web

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	No				x	x	Es necesario que se establezcan acuerdos con el proveedor de la aplicación para el tratamiento de la seguridad de la información especialmente con los datos que contienen identificación personal.
	15.1.3	Cadena de suministro de tecnología de información y comunicación					x	x	se necesita implementar dentro de los acuerdos con los proveedores los requisitos para tratar los riesgos de la seguridad de la información relacionados con los procesos logísticos realizados
	15.2	**Gestión de la prestación del servicios de proveedores**							
	15.2.1	Seguimiento y revisión de los servicios de los proveedores					x	x	Se debe hacer un seguimiento periódico que permita verificar los servicios prestados por el proveedor.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	15.2.2	Gestión de cambios en los servicios de los proveedores					x	x	Es necesario gestionar los cambios o modificaciones de los servicios de acuerdo a los niveles de importancia de la información
16 Gestión de los incidentes de la seguridad de la información	**16.1**	**Gestión de los Incidentes y las Mejoras en la Seguridad de la Información**							
	16.1.1	Responsabilidades y procedimientos					x	x	Cuando se presenten incidentes de seguridad de la información la institución debe estar preparada para dar una solución oportuna, para ello se debe haber establecido los procedimientos y responsabilidades necesarias.
	16.1.2	Reporte sobre los eventos de seguridad de la información					x	x	Para los incidentes presentados en la seguridad de la información es de vital importancia la gestión de los riegos y este debe poseer un canal eficaz que permita comunicar oportunamente los incidentes presentados.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									para que sean solucionados con rapidez
	16.1.3	Reporte sobre las debilidades en la seguridad					x	x	Los usuarios de la institución deben reportar de forma eficaz cualquier evento o debilidad identificada y que ponga en riesgo la seguridad de la información usando los canales de gestión para su comunicación.
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos					x	x	Se deben establecer controles para la evaluación de los incidentes de la seguridad de la información, su clasificación, análisis y acción de mejora.
	16.1.5	Respuesta a incidentes de seguridad de la información					x	x	De acuerdo a los controles que establecidos para los incidentes de seguridad de la información se deben hacer a través de procedimientos documentados.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información					x	x	En la medida en la que se conozcan los diferentes incidentes de seguridad de la información presentados en la institución, su análisis y la forma de solucionarlos le permitirá al área encargada adquirir un conocimiento adicional para reducir incidentes futuros.
	16.1.7	Recolección de evidencias	x				x	x	Se deben establecer procedimientos para la relección de evidencias para que estas sean válidas para poder realizar las diferentes acciones disciplinarias y legales sobre dicho incidente.
17	**17.1**	**Continuidad de seguridad de la información**							
	17.1.1	Planificación de la continuidad de la seguridad de la información	x				x	x	La institución después de determinar las necesidades de la seguridad de la información debe implementar un plan de

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Apli ca	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Cont rol**				**L R**	**C O**	**BR/ BP**	**RR A**	
Aspectos de seguridad de la informaci ón de la gestión de la continuid ad del negocio									Continuidad de la gestión de la seguridad de la información para las situaciones complejas que presente en su capacidad de ejecución o recuperación de desastres.
	17.1. 2	Implementació n de la continuidad de la seguridad de la información	x				x	x	La institución necesita establecer procedimientos y controles documentados, para la gestión de la seguridad, cuando se presenten situaciones complejas que comprometan la seguridad de la información y su correcto funcionamiento
	17.1. 3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	x				x	x	Es importante para la institución que después de haber identificado, establecido los procesos e implementados adecuadamente al plan de continuidad, junto con los procesos, controles para

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
									que estos sean revisados, verificados y evaluados en intervalos establecidos cumpliendo con los requisitos de la seguridad de la información.
	17,2	**Redundancias**							
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	x						
18 Cumplimiento	**18.1**	**Cumplimiento de los Requisitos Legales y Contractuales.**							
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	x		x	x	x	x	La institución debe verificar que cumple con los requisitos enviados por medio de resoluciones en donde se especifican el cumplimiento de normas concretas y deben estar documentados y actualizados.

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
	18.1.2	Derechos de propiedad intelectual (DPI)	x		x	x	x	x	La institución debe tener conocimiento sobre los derechos de propiedad intelectual según lo establecido en la norma, para poder así establecer las políticas de seguridad en el uso legal del software y los productos de información.
	18.1.3	Protección de registros	x		x		x	x	Para la protección de los registros es necesario que la institución realice una clasificación para que puedan ser categorizados y especificados sus procedimientos y los medios de almacenamiento aplicado, sus claves criptográficas y programas de encriptado para los archivos.
	18.1.4	Privacidad y protección de información de	x				x	x	La institución maneja una cantidad considerable de información relacionada con los datos personales, por lo

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	**Control**				**LR**	**CO**	**BR/BP**	**RRA**	
		datos personales							cual debe establecer una política que dé cumplimiento a la ley de la protección de datos, dicha política debe darse a conocer a sus usuarios.
	18.1.5	Reglamentación de los controles criptográficos	x						La institución debe establecer reglamentos a los controles criptográficos basados en el cifrado de contraseñas o de información sensible que ponga en riesgo la seguridad de la información, además se debe tener en cuenta el cumplimiento de las leyes pertinentes.
	18.2	**Revisiones de seguridad de la información**							
	18.2.1	Revisión independiente de la seguridad de la información	x				x	x	Se deben realizar auditorías externas periódicas que permitan evaluar en todos los procesos la seguridad de la información y pueda sugerir mejoras que

Tabla 23. (Continuación)

ISO/IEC 27001:2013 Anexo A controles			Aplica	justificación de las exclusiones	controles seleccionados				justificación de la elección del control
Sección	Control				LR	CO	BR/BP	RRA	
									contribuyan con el objetivo principal de la institución.
	18.2.2	Cumplimiento con las políticas y estándares de seguridad	x				x	x	La institución debe garantizar la seguridad de la información que se implementa y opera de acuerdo con las políticas y procedimientos establecidos
	18.2.3	Revisión del cumplimiento técnico	x				x	x	Se debe realizar la revisión del cumplimiento técnico mediante informes que reflejen el uso de las herramientas idóneas y las evidencias encontradas en su análisis.

Fuente: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf y el autor.

13.1. NO CONFORMIDADES DE LA INSTITUCIÓN EDUCATIVA

Después de realizar la declaración de aplicabilidad conforme al anexo A de la norma ISO 27001 en donde se identificó los controles que aplican a la institución educativa y los que se excluyen, se procede a realizar una no conformidad en donde se especifica que controles la institución está incumpliendo en el proceso gestión académica como se explica a continuación

- Se evidencia que la institución está incumpliendo la cláusula 5. Políticas de seguridad la institución en los numerales 5.1.1 y 5.1.2 ya que de acuerdo a la lista de chequeo y la entrevista realizada según los anexos C y D a los actores del proceso y la visita realizada a la institución, se evidencia que esta no cuenta con políticas de seguridad en el proceso gestión académica y el personal maneja la información de a criterio personal o bajo algunas recomendaciones verbales impartidas por el coordinador, lo cual pone en riesgo la información sensible como por ejemplo los formatos de inscripción, los formatos de matrícula, las constancias académicas, los informes de periodo, los formatos de calificaciones, registro en el simat y la información de la aplicación web, esta no conformidad es de tipo mayor.

- El control 6.1.1 Roles y responsabilidades para la seguridad de la información; es incumplido en la institución, según la entrevista realizada a los actores principales del proceso gestión académica Anexo D, ya que no existen documentos que especifiquen los roles y responsabilidades de la seguridad de la información para los docentes, la secretaria y el coordinador que son los implicados en la realización de los procedimientos , ellos afirman que conocen superficialmente algunos los roles y responsabilidades y que estos fueron socializados de forma verbal, al conocer los roles y responsabilidades de forma parcial y verbalmente, algunas veces se incurre en omisión de algunas responsabilidades en el proceso, lo que atrasa las actividades realizadas, esta no conformidad es de tipo mayor.

- En la institución no se está aplicando el numeral 8.2.1 clasificación de la información, según el resultado de la lista de chequeo correspondiente al anexo C, se evidencia que en los procedimientos de matrícula e inscripción, registro de estudiantes en el simat, registro de calificaciones y generación de certificados y constancias, no se realiza una clasificación de la información adecuada conforme a la norma ISO 27001, dicha clasificación solo se realiza teniendo en cuenta la fecha y los cursos correspondientes al año lectivo sin tener en cuenta su sensibilidad o nivel de criticidad, esta no conformidad es de tipo mayor.

- El control 8.2.2 Etiquetado de la información, por medio de la visita a las instalaciones y a la lista de chequeo realizada, se identificó que se incumple dicho control ya que en la información física que maneja la secretaria y que es guardada en los archivadores, contiene una etiqueta clasificada solo por grado y fecha, sin tener en cuenta los niveles de confidencialidad y disponibilidad e integridad, de igual forma la información digital en los equipos de los docentes carece de tanto de clasificación como de etiquetado, esta es guardada sin ningún tener en cuenta los parámetros de seguridad y sus niveles. Esta conformidad es de tipo mayor.

- El numeral 9.1.1 Política de control de acceso: la institución no cumple con dicho control ya que con la entrevista realizada a los actores principales del proceso y la visita a las instalaciones , se logró identificar que los docentes, el coordinador y la secretaria, en los computadores asignados a cada uno no cuentan con perfiles de usuario para los equipos que manejan, de esta forma cualquier persona puede acceder a la información almacenada en el equipo, también se evidencio que en estos equipos los usuarios tienen acceso a todo, es decir no tienen limitaciones o restricciones de acceso a aplicaciones y servicios, esta no conformidad es de tipo menor.

- El control 9.1.2 Acceso a redes y a servicios de red: es incumplido en la institución conforme a la verificación correspondiente a la lista de chequeo del Anexo C, los usuarios no tienen restricciones a la red ni a los servicios de red, ya que pueden realizar descargas desde diferentes sitios, ingresar a todas las páginas que el usuario desee, y no está establecido la seguridad para la red Wifi, lo que pone en riesgo la seguridad de la información y la productividad de los procedimiento realizados en la gestión académica. esta no conformidad es de tipo menor.

- En la aplicación web libreta escolar los usuarios manejan contraseñas para ingresar al sistema, estas son débiles y no cumplen con los requisitos mínimos aunque su longitud es de más de 8 caracteres, estas no contienen letras mayúsculas, números y caracteres especiales , se evidenció también que la vigencia de estas contraseñas es de 12 meses lo cual es un periodo muy prolongado, ya que las contraseñas deben ser cambiadas cada tres meses, el cambio de contraseñas es enviado al correo de los usuarios sin ningún tipo de seguridad, de esta forma en dicho procedimiento se está incumpliendo con el control 9.4.3 Sistema de gestión de contraseñas. Esta no conformidad es de tipo menor.

- La institución está incumpliendo el control 10.1 Política sobre el uso de controles criptográficos, ya que en el análisis de la aplicación web se evidencia que la información sensible producida en dicha aplicación , como por ejemplo; los boletines de cada periodo académico que son

generados en un PDF no tienen ninguna restricción para ser descargados y visualizados, tampoco están protegidos contra modificaciones y permiten fácilmente cambiar el formato PDF a Word sin mayor esfuerzo, en los demás procedimientos los docentes, la secretaria y el coordinador realizan envíos de boletines, listados de notas, certificados y constancias a través del correo y dicha información no cuenta con ninguna técnica de cifrado o llaves criptográficas, debido a esto la información sensible puede ser robada, eliminada o modificada poniendo en riesgo la confidencialidad e integridad de la información, esta no conformidad es de tipo mayor.

- El control ubicado en el numeral 11.2. Servicios de suministro, de acuerdo a la visita realizada a las instalaciones de la institución se evidencia que esta no cuenta con un servicio de suministro en caso de fallas o suspensión del servicio de energía, lo que puede provocar una interrupción en los procedimientos realizados en los equipos, como el registro de calificaciones en la aplicación web, la realización de constancias y certificados, el registro de estudiantes en el simat que hacen parte del proceso de gestión académica, estas interrupciones ocasionan atrasos en los cronogramas establecidos para el cumplimiento de las actividades. Esta no conformidad es de tipo menor.

- En la entrevista realizada a los actores principales del proceso gestión académica y la visita a las instalaciones se identificó que los computadores usados para dicho proceso no cuentan con un mecanismo de bloqueo cuando el usuario desatiende dicho equipo, además sus terminales tampoco están protegidos contra usos no autorizados, exponiendo de forma significativa la información sensible almacenada en los equipos e incumpliendo con el control 11.2.8 Equipo de usuario desatendido, esta no conformidad es de tipo mayor.

- El control 11.2.9 Política de escritorio despejado y de pantalla despejada se está incumpliendo en la institución ya que se encontró sobre el escritorio de trabajo de la secretaria y del coordinador diferentes documentos como boletines, constancias, certificados que son confidenciales y que pertenecen al proceso de gestión académica que pueden estar expuesto a robo, eliminación o modificación , también incumplen tanto los docentes, la secretaria y el coordinador con el objetivo de pantalla despejada de este control, ya que se encontró en 10 equipos archivos de información personal, y equipos desatendidos que no cuentan con un mecanismo de bloqueo como se mencionó en la no conformidad del control anterior. esta no conformidad es de tipo menor.

- El control de acceso contra código malicioso de la norma ISO 27001 descrito en el numeral 12..2.1, según la entrevista y la lista de chequeo realizado en la institución, se identificó que se incumple con este control ya que en los computadores de la secretaria, el coordinador y los

docentes, pueden descargar e instalar desde internet software no autorizado, debido a que no cuenta con restricciones de instalación , ni restricciones a paginas o servicios de internet, además la institución no cuenta con un procedimiento para el uso del antivirus en caso de algún ataque, esta no conformidad es de tipo menor.

- La institución incumple con el numeral 12.3.1 Copias de respaldo de la información, de acuerdo al análisis realizado a la aplicación web se identificó que esta realiza una copia de seguridad cada semana en el servidor web, a estas copias solo tienen acceso los proveedores de la aplicación web y cuando se han presentado inconvenientes con la información se deben poner en contacto con los proveedores para que ellos den solución basados en las copias de seguridad realizadas, en los demás procedimientos pertenecientes a la gestión académica, no se realizan copias de seguridad , de esta manera la información que esta almacenada en los equipos en caso de ser afectada se corre el riesgo de perder la disponibilidad y la integridad de la información. esta no conformidad es de tipo mayor.

- Para el caso de la Instalación de software en sistemas operacionales correspondiente al numeral 12.3.5, de acuerdo a la lista de chequeo realizada se evidencio que Los usuarios del proceso gestión académica pueden realizar instalaciones de software en sus equipos ya que estos no cuentan con las restricciones de instalación adecuadas , algunos docentes llevan los instaladores de software en memorias USB, otros los descargan desde internet, además los usuarios no realizan ningún tipo de notificación o solicitud de aprobación para que dichas instalaciones sean evaluadas si son necesarias o no, para el desempeño de las funciones asignadas en el proceso gestión académica. esta no conformidad es de tipo menor.

- El control 12.7.1 Controles de auditorías de sistemas de información se evidencio que la institución no cuenta con un plan de auditoria para el proceso de gestión académica que especifique los requisitos y controles necesarios para que no se interrumpan las actividades realizadas. Esta conformidad es de tipo menor.

- Políticas y procedimientos para el intercambio de información; corresponde al control número 13.2.1 de la norma, según el análisis realizado al proceso gestión académica se identificó que se incumple con este numeral ya que hay intercambio de información entre secretaria, coordinador y docentes por medio del correo electrónico y dicho intercambio no cuenta con ningún control de seguridad que evite la fuga, el copiado o perdida de la información, ya que los archivos enviados

pueden ser descargados y no tienen ninguna restricción de edición. Esta no conformidad es de tipo mayor.

- Según las entrevistas realizadas a los actores principales del proceso gestión académica se identificó que se le han realizado cambios a la aplicación web de forma paulatina desde su adquisición, para que esta se adapte a las necesidades de la institución, dichos cambios realizados no han sido documentados omitiendo la verificación del cumplimiento de la seguridad de la información de la aplicación web y de esta forma incumpliendo el control 14.2.1 Política de desarrollo seguro. Esta no conformidad es de tipo menor.

- La institución incumple el control 16. Gestión de los incidentes de la seguridad de la información**,** desde el numeral 16.1.1 al 16.1.7 ,en donde se logró identificar que no están preparados en caso de que se presenten incidentes a la seguridad de la información, ya que no hay documentación donde se hayan establecido procedimientos para detectar posibles incidentes en la gestión académica, los pasos adecuados para su tratamiento, su evaluación y acción de mejora que eviten futuros incidentes que puedan afectar los procedimientos de la gestión académica y la disponibilidad y confidencialidad de la información. Esta no conformidad es de tipo mayor

- Planificación de la continuidad de la seguridad de la información que describe el numeral 17.1.1 se evidencia en la lista de chequeo realizada que este control es incumplido en la institución ya que no posee controles para la continuidad de la información en caso de que se presenten situaciones adversas, la institución no ha realizado el análisis de los posibles riesgos y las acciones preventivas que permitan reducirlos a través de los planes de seguridad de la información y su debida actualización. Esta no conformidad es de tipo menor.

- La institución maneja una cantidad considerable de información relacionada con los datos personales de los estudiantes y de acuerdo a las entrevistas realizadas se desconoce la forma y los lineamientos legales para el tratamiento que se le debe dar a los datos personales manejados en el proceso gestión académica, su almacenamiento y custodia, motivo por el cual no está cumpliendo con el control 18.1.4 Privacidad y protección de información de datos personales. Esta no conformidad es de tipo menor.

14. INFORME Y RECOMENDACIONES

En el análisis realizado al proceso gestión académica se identificaron 20 no conformidades, 9 de tipo mayor y 11 no conformidades de tipo menor como se describen a continuación:

No conformidades de tipo mayor

- **Políticas de seguridad de la información y revisión de estas; recomendación:** la institución debe establecer una política de seguridad de la información teniendo en cuenta sus objetivos y requisitos legales, este procedimiento debe ser documentado, posteriormente se deben socializar a los docentes, el coordinador y secretaria acompañada de una capacitación sobre la importancia de la seguridad de la información para la institución, además se debe programar una revisión periódica de las políticas establecidas con su correspondiente registro.

- **Roles y responsabilidades para la seguridad de la información**; **recomendación**: la institución debe documentar las funciones y responsabilidades de la seguridad de la información en el proceso gestión académica para los docentes, secretaria y coordinador, socializarlas con sus actores y posteriormente monitorear que el SGSI cumple con lo establecido en la norma.

- **clasificación de la información; recomendación:** se debe realizar un inventario de activos del proceso gestión académica identificando a sus responsables, después se debe realizar una clasificación de acuerdo a los diferentes niveles de confidencialidad de la información que maneja la institución, por ejemplo se pueden establecer niveles de confidencialidad alta, media, baja y pública.

- **Etiquetado de la información**; **recomendación:** De acuerdo a la clasificación realizada la institución deberá realizar un etiquetado de la información física para lo cual se recomienda usar un sello, para la información digital y para los activos tecnológicos.

- **Política sobre el uso de controles criptográficos; recomendación**: la institución debe establecer controles criptográficos teniendo en cuenta tanto la clasificación de la información como las técnicas de cifrado que serán usadas, la gestión de claves y generación de claves y los roles y responsabilidades de los encargados.

- **Equipo de usuario desatendido; recomendación:** se debe implementar un sistema de bloqueo de pantalla por medio de contraseñas para la

seguridad de los equipos desatendidos, bloqueando el ingreso al sistema, y los puertos del equipo.

- **Copias de respaldo de la información; recomendación:** la institución debe elegir un software para la realización de copias de respaldo de la información, y elegir a la persona encargada de este procedimiento a la información sensible del proceso académico previamente identificada, como archivos confidenciales, aplicaciones, correo, impresiones, base de datos entre otros, también debe establecer los intervalos de tiempo en los que se realizaran las copias de respaldo indicando fecha, hora exacta y el lugar donde será almacenada, se debe verificar que las copias realizadas son correctas y que se puede hacer una restauración correctamente si se requiere.

- **Políticas y procedimientos para el intercambio de información: recomendación:** se le indica a la institución que debe establecer políticas para el intercambio de información ya que en el proceso gestión académica hay envío y recepción de información sensible como registro de notas, informes de periodo, certificados, esta información sensible debe ser cifrada y protegida contra escritura para que no se puedan realizar modificaciones, los empleados deben conocer las políticas y procedimiento y la importancia que tienen para la seguridad de la información del proceso gestión académica.

- **Gestión de los incidentes de la seguridad de la información; recomendación:** Es importante que la institución establezca un procedimiento para la gestión de incidentes del proceso gestión académica que permita solucionarlos de forma eficaz y eficiente, los empleados deben conocer dichos procedimientos para que puedan ponerse en práctica, en primera instancia debe haber una comunicación del incidente, posteriormente se debe clasificar

No conformidades de tipo menor

- **Política de control de acceso: recomendación:** la institución debe establecer controles basados en las responsabilidades y roles asignados a sus empleados para poder crear para cada uno perfiles de usurarios y le sean otorgado permisos de acuerdo a su perfil y con un nivel de acceso diferente para cada usuario.
- **Acceso a redes y a servicios de red; recomendación:** Se debe establecer controles para permitir la conexión a dominios específicos teniendo en cuenta los roles y responsabilidades de cada usuario del proceso gestión académica, también se recomienda implementar

controles de direccionamiento que permitan confirmar las direcciones de origen y destino de las conexiones realizadas en la red.

- **Sistema de gestión de contraseñas; recomendación:** Se deben establecer perfiles de usuario y los accesos según sus roles y responsabilidades, implementar un proceso de eliminación de derechos de acceso en caso de que un usuario salga de su cargo, crear políticas de control de acceso y contraseñas y socializarlas con los usuarios.

- **Servicios de suministro, recomendación:** Se recomienda que la institución adquiera UPS para los equipos usados en el proceso de gestión académica por docentes, coordinador y secretaria.

- **Política de escritorio despejado y de pantalla despejada**; **recomendación:** Es necesario que los usuarios cuando se ausenten de su lugar de trabajo dejen su equipo bloqueado evitando riesgos en la seguridad de la información, también debe guardar bajo llave cualquier documento que contenga información sensible.

- **El control de acceso contra código malicioso; recomendación:** La institución debe implementar políticas de licencias de software e instalación, revisiones periódicas para la actualización de antivirus, usar para los correos electrónicos el antivirus para la verificación de los archivos adjuntos recibidos, la institución debe socializar y capacitar a los usuarios sobre estas políticas implementadas.

- **Instalación de software en sistemas operacionales; recomendación:** La institución debe establecer reglas para la instalación de software, en donde los usuarios deben realizar una solicitud a la directiva y esta debe quedar registrada, se evaluara la instalación es requerida para las responsabilidades asignadas y si cuenta con la licencia necesaria para su instalación.

- **Controles de auditorías de sistemas de información; recomendación:** La institución debe establecer los controles que deben tener las auditorías al sistema de información para que no se entorpezcan las actividades realizadas.

- **Política de desarrollo seguro; recomendación:** Para la aplicación web y para cualquier procedimiento que se modifique en el proceso académico, debe llevar una documentación que permita corroborar que dicho cambio no altera las actividades realizadas, las modificaciones deben ser socializadas con los usuarios.

- **Planificación de la continuidad de la seguridad de la información; recomendación:** La institución debe implementar un plan de continuidad

de la información que permita adaptarse a las modificaciones de los procedimientos y no se altere la seguridad de la información, teniendo también en cuenta que ante los incidentes que se puedan presentar se debe tener un nivel aceptable para la seguridad de la información del proceso gestión académica.

- **Privacidad y protección de información de datos personales: recomendación:** es necesario que la institución se encargue de conocer la Política de Privacidad y Protección de Datos Personales de acuerdo a "la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013"[12], para poder darle el tratamiento correspondiente a los datos personales de los estudiantes y sus acudientes.

En la siguiente tabla se establecerá un cronograma para que la institución realice las recomendaciones hechas a las no conformidades encontradas.

Tabla 30. Plan de acción recomendado

PLAN DE ACCIÓN RECOMENDADO												
Actividades	**Mes 1**				**Mes 2**				**Mes 3**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**3**	**1**	**2**	**3**	4
Políticas de seguridad de la información y revisión de estas												
Roles y responsabilidades para la seguridad de la información												
clasificación de la información; recomendación												
Etiquetado de la información												
Política sobre el uso de controles criptográficos												
Equipo de usuario desatendido												
Copias de respaldo de la información												

[12] https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

PLAN DE ACCIÓN RECOMENDADO												
Actividades	**Mes 1**				**Mes 2**				**Mes 3**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**3**	**1**	**2**	**3**	4
Políticas y procedimientos para el intercambio de información												
Gestión de los incidentes de la seguridad de la información												
Política de control de acceso												
Acceso a redes y a servicios de red; recomendación												
Acceso a redes y a servicios de red												
Sistema de gestión de contraseñas												
Servicios de suministro												
Política de escritorio despejado y de pantalla despejada												
El control de acceso contra código malicioso												
Instalación de software en sistemas operacionales												
Controles de auditorías de sistemas de información												
Política de desarrollo seguro												
Planificación de la continuidad de la seguridad de la información												
Privacidad y protección de información de datos personales												

15. Conclusiones

El proyecto realizado permitió identificar diferentes criterios esenciales en la seguridad de la información y el conocimiento detallado de la norma ISO 2700; 2013 y la importancia de la aplicación de los controles en una organización y los elementos necesarios para realizar un análisis y posterior diagnóstico de la Institución en mención.

De acuerdo a los resultados arrojados en el desarrollo del proyecto se puede decir que la falta de conocimiento sobre la importancia de la seguridad de la información, como uno de los mayores activos de la organización, conlleva a un conjunto de malas prácticas dentro de los procedimientos realizados, de omisión de responsabilidades en los diferentes cargos por desconocimiento o por la falta de implementación de políticas de seguridad que permitan proteger adecuadamente la información del proceso gestión académica.

Finalmente después de diagnosticar el estado actual de la institución basado en la norma ISO 27001 en donde se hallaron no conformidades de tipo mayor y menor se hace una recomendación a la institución con el fin de que se realice una mejora a la seguridad de la información en el proceso seleccionado.

16. BIBLIOGRAFÍA

Calderon Hugo, Metodologia de la investigación cientifica, Tipos de investigación 2014, UNIVERSIDAD NACIONAL DEL SANTA Escuela Académica Profesional Ingeniería en Energía, Disponible en: http://biblioteca.uns.edu.pe/saladocentes/archivoz/curzoz/002_clase4.pdf

Codejobs, Auditoria informática, ¿Qué es una auditoria informatica , 2015 ,disponible en: https://www.codejobs.biz/es/blog/2013/02/25/que-es-una-auditoria-informatica.

Cristian Boghello, Cambios y mapeo de controles ISO 27001: 2013, 2014 disponible en: http://www.segu-info.com.ar/boletin/boletin-199-140714.htm

Dejan Kosutic, la importancia de la declaración de aplicabilidad para la norma iso 27001, 2015. Disponible en: https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/ .

Dirección General de Modernización Administrativa, P. e.. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre de 2012, Libro II. Madrid: © Ministerio de Hacienda y Administraciones Pública.

FACULTAD DE CIENCIAS EMPRESARIALES, Obtenido de http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

Gerencie, Gerencia Auditoria de sistemas de información, Planeación de una auditoria informática, 2013, INSTITUCIÓN UNIVERSITARIA DE ENVIGADO

Grajales Tevni, Tipos de investigación, Formas de clasificación de las investigaciones, 2000, Disponible en: http://tgrajales.net/investipos.pdf

Guindel Esmeralda, Calidad y seguridad de la información y auditoría informática, calidad y seguridad de la informacion,2010, Trabajo de grado (ingeniería técnica de informática de gestión), Universidad Carlos III de Madrid Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence=1

Jimenez Lina, Tenología Informática, Técnicas de recolección de información, 2012, INSTITUCIÓN PEDRO OCTAVIO AMADO, Disponible en:

http://es.slideshare.net/linajimenez30/guia1-tcnicas-de-recoleccion-de-informacin.

Journal Isaca, Vulnerabilidades, Riesgo asociado con las aplicaciones web, 2009, CASCHILE, Disponible en: http://www.bscconsultores.cl/descargas/B.2%20Vulnerabilidad.pdf

Ludewig Cristina, Universo y muestra, Caracteristicas de una buena muestra,2014, Disponible en: http://www.smo.edu.mx/colegiados/apoyos/muestreo.pdf

LUGO MENDEZ LUZ MARIA, Auditoria Informática,Fases de la auditoria ,2011, INSTITUTO TECNOLÓGICO DE TIJUANA Subdirección Académica Departamento de Sistemas y Computación Licenciatura en Informática, Disponible en: http://es.slideshare.net/Luzah/fases-de-la-auditora.

Manuel collazos B, La nueva versión ISO 27001:2013 un cambio en la integración de los sistemas de gestión, 2014 disponible en:

Mejia Cuellar Guillermo, Planeación de auditoria, Importancia de la planeación,2009, Teoria General de la Auditoria, Disponible en: https://preparatorioauditoria.wikispaces.com/file/view/Unidad+Seis.pdf

Mendoza Miguel, Identificación y análisis a la gestión de riesgos de seguridad,Gestion de riesgos de seguridad, 2015, Welyvetsecurity, Disponible en: http://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad/

Mifsud Elvira, Introducción a la Seguridad Informática,Seguridad de la información / Seguridad informática, 2012, Observatorio Tecnológico, Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

Mifsud Elvira, Introducción a la Seguridad Informática,Vulnerabilidades de un sistema informàtico,2012, Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Mosquera , Riesgosy control informático, Fases de la auditoria informatica y de sistemas,2014, Universidad Nacional Abierta y a Distancia unad, Ingenieria de sistemas,Disponible en:

http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_27_fases_de_la_auditora_informtica_y_de_sistemas.html.

Quality & Performance Management, Calidad y excelencia, Dominios tecnologicos de la seguridad de la información ISO 27001, 2013,IsoTools excelence, Disponible en : https://www.isotools.org/2013/10/03/iso-27001-dominios/. (s.f.).

ticbogota.gov.co/sites/default/files/.../AutodiagnosticoSGSI_v2_09072015.xls?.

UIAF, Ley estatutaria 1266, 2008 Unidad de Información y analisis financiero republica de Colombia, Disponible en: https://www.uiaf.gov.co/?idcategoria=20630.

ANEXOS

Anexo A. Encuesta

CONOCIMIENTO DE LA INSTITUCION EDUCATIA SEDE MERCEDES PARDO DE SIMMONDS

FECHA: _____

INFRAESTRUCTURA

- ¿El establecimiento es propio? : si _____ no_____
- ¿Cuantas oficinas tiene la institución?: _____
- ¿Cuantas aulas de clase tiene la institución?: _____

ORGANIZACIÓN

- ¿Cuáles son las actividades realizadas en el proceso gestión académica?: _____ _____ _____ _____ _____
- ¿Cuántos docentes hay en la institución?: _____
- ¿Cuántos administrativos hay la institución?: _____

SERVICIOS

- ¿El establecimiento posee servicio de internet? : si _____ no_____
- ¿Cuál es el proveedor del servicio de internet? :_____
- ¿El establecimiento posee servicio de telefonía? : si _____ no_____
- ¿Cuál es el proveedor del servicio de telefonía? :_____
- ¿El establecimiento cuenta con alguna aplicación web? : si ___ no_____
- ¿Cuál es la función de la aplicación web? _____ _____
- ¿El establecimiento posee servicio de televisión? : si ____ no_____
- ¿Cuál es el proveedor del servicio de televisión? :_____

.

Anexo B. Lista y descripción de inventario

OFICINA RECTORIA			
CANTIDAD	DESCRIPCION	FINALIDAD	ENCARGADO
1	Computador de mesa hp	Reportes, informes	Rector
1	Impresora Epson	Impresiones rectoría	Rector
1	Modem	Conexión a internet	Rector

OFICINA ADMINISTRATIVO			
CANTIDAD	DESCRIPCION	FINALIDAD	ENCARGADO
1	Computador de mesa hp	Reportes, informes	Secretaria
1	Impresora Epson	Impresiones rectoría	Secretaria
1	Modem	Conexión a internet	Secretaria

AULAS DE CLASE			
Nº	DESCRIPCIÓN	FINALIDAD	ENCARGADO
10	Computador de mesa hp	Reportes, informes, listados, calificaciones	Docentes
1	Impresora Epson	Impresiones Docentes	Docentes
10	Televisor lg plasma	Proyección de videos, imágenes en el aula.	Docentes

SALA DE INFORMATICA			
Nº	DESCRIPCIÓN	FINALIDAD	CATEGORIA
40	Computador portátil pc Smart	Uso de estudiantes área tecnología e informática	Docente
1	Impresora Epson	Impresiones estudiantes	Docente
1	Cabina activa DJ pro	Audio sala informática	Docente
1	Video beam Lg	Proyecciones sala informática	Docente

Anexo C. lista de chequeo docentes, secretaria y coordinador.

ITEM A EVALUAR	**Cumple**	**Cumple parcialmente**	**No cumple**
Los equipos asignados están bajo la responsabilidad de cada docente.			
Las aulas donde están los equipos cuentan con seguridad necesaria.			
cuenta con un usuario y contraseña en el equipo			
puede instalar programas en el equipo sin restricciones			
Se realizan mantenimientos preventivos periódicamente			
Se realizan mantenimientos correctivos periódicamente			
Se hacen copias de seguridad en los equipos			

ITEM A EVALUAR	Cumple	Cumple parcialmente	No cumple
Los equipos cuentan con ups			
Hay control de acceso de personal no autorizado			
Existen políticas para el manejo de los equipos			
Tiene conexión a internet			
El servicio de internet funciona correctamente			
Tiene restricciones para ingresar algunas páginas de internet			
El aula de clase y oficina cuenta con prevención contra inundación.			

Anexo D. Cuestionario hardware control e inventario de equipos proceso gestión académica.

CUESTIONARIO PARA HARDWARE			
Dominio	Adquisición e Implementación		
Proceso	Adquirir y mantener la arquitectura tecnológica		
Pregunta	**Si**	**No**	**OBSERVACIONES**
¿Se cuenta con un inventario de equipos de cómputo?			
¿Si existe inventario contiene los siguientes ítems? Número del computador			
Fecha			
Ubicación			
Responsable			
Características(memoria, procesador, monitor, disco duro)			
Se lleva una hoja de vida por equipo			

¿La hoja de vida del equipo tiene los datos? Numero de hoja de vida			
Número del computador correspondiente Falla reportada			
Diagnóstico del encargado			
Solución que se le dio			
¿Se posee un registro de fallas detectadas en los equipos?			
¿En el registro de fallas se tiene en cuenta con los siguientes datos? Fecha			
Hora			
Número de registro			
Número del computador			
Encargado			
¿Al momento de presentar una falla en el equipo, la atención que se presta es? Inmediata			
De una a 24 horas			
De un día a 5 días Más de 5 días			
¿Se cuenta con servicio de mantenimiento para todos los equipos?			
¿Qué tipo de mantenimiento se lleva a cabo? Mantenimiento preventivo			
Mantenimiento correctivo			
¿Profesores pueden instalar y desinstalar programas en el computador?			
¿Al finalizar el horario de clase en dichas aulas, se hace una revisión de los equipos?			
¿El personal que se encarga del mantenimiento es personal capacitado?			
¿Se lleva un procedimiento para la adquisición de nuevos equipos?			
¿La infraestructura tecnológica de los equipos soporta la instalación de diferentes sistemas operativos?			
¿Son compatibles software y hardware?			

Anexo E. Lista de chequeo aplicación web.

ITEM A EVALUAR	Cumple	Cumple parcialmente	No cumple
Conoce las responsabilidades de seguridad de la información de la aplicación web.			
Tiene una contraseña segura para ingresar a la aplicación web.			
El cambio de contraseña es realizado cada tres meses.			
La información está clasificada según su criticidad o confidencialidad.			
La información está etiquetada de acuerdo a su clasificación.			
La información sensible del proceso gestión académica cuenta con cifrado.			
Se hacen copias de seguridad			

Resumen analítico RAE

Título de Documento.	DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL SEDE MERCEDES PARDO DE SIMMONDS DE LA CIUDAD DE POPAYÁN.
Autor	RESTREPO SANTARUZ Jenny Fernanda
Fuentes Bibliográficas	Calder, A., & Watkins, S. G. (2010). Information Security Risk Management for ISO27001/ISO27002. Cambridgeshire: IT Governance Publishing. Dejan Kosutic, la importancia de la declaración de aplicabilidad para la norma iso 27001, 2015. Disponible en: https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/ .. Watkins, S. G. (2008). An Introduction to Information Security and ISO 27001. Ely: IT Governance Publishing.
Año	2018
Resumen	Para el desarrollo del diagnóstico se realizará la recolección de información de las áreas adyacentes al proceso gestión académica, con el fin de identificar los activos de información que hacen parte del proceso y detectar las amenazas, vulnerabilidades y riesgos por medio de una revisión basada en el estándar ISO 27001:2013, con dicha recolección de información y posterior detección de riesgos se procederá a establecer los controles necesarios de acuerdo a la declaración de aplicabilidad extraída en el anexo A ISO 27001 ,una vez identificados los controles que no se están cumpliendo se procederá a dar la respectivas recomendaciones para lograr el cumplimiento de los mismos
Palabras claves	Seguridad de la información, proceso, ISO 27001:2013, vulnerabilidades, riesgos., políticas de seguridad, controles.
Contenidos	1. INTRODUCCIÓN 2. PLANTEAMIENTO DEL PROBLEMA 3. OBJETIVOS 4. JUSTIFICACIÓN

	5. ALCANCE Y DELIMITACIÓN DEL PROYECTO 6. MARCO REFERENCIAL 7. MARCO METODOLÓGICO 8. DESARROLLO DEL PROYECTO 9. INFORME Y RECOMENDACIONES Conclusiones 10. BIBLIOGRAFÍA 11. ANEXOS

Descripción del problema

La Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds, es una institución que ofrece sus servicios educativos a 520 estudiantes, sus instalaciones físicas cuentan con los requerimientos necesarios para la educación de los niños, además cuenta con equipos tecnológicos de última generación tales como una sala de tecnología e informática dotada de 40 computadores portátiles, 10 computadores de mesa video beam, micrófono inalámbrico, cabina activa, sala de audiovisuales, la institución cuenta con un servicio de internet de 20 Gb.

A pesar de que la institución educativa cuenta con las herramientas tecnológicas adecuadas para optimizar su progreso a nivel educativo y administrativo, este no cuenta con un sistema que garantice la seguridad de la información, motivo por el cual está en riesgo eminente debido a la cantidad de información que se maneja en el proceso de gestión académica; como el ingreso de calificaciones, creación de logros e indicadores de logro, por periodos académicos establecidos por la institución, generación de informes de calificaciones de cada estudiante información que es creada y modificada por medio de una aplicación web, la cual no cuenta con las políticas de seguridad adecuadas, aunque cuenta con contraseñas de usuario estas no están cifradas, los certificados emitidos por la institución no cuentan con la seguridad necesaria de un documento digital.
Lo que se busca en la Institución es realizar en primera instancia un diagnostico al estado actual de la seguridad informática basada en el estándar ISO 27001:2013 que permita identificar las vulnerabilidades, amenazas y riesgos a los que está expuesta la institución educativa en el proceso de gestión académica.

Objetivos

OBJETIVO GENERAL

Realizar un diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013 que le brinde a la institución educativa el contexto de cómo está tratando la seguridad de la información y las mejoras que se pueden implementar en su proceso.

OBJETIVOS ESPECÍFICOS

Identificar los procedimientos actuales de la institución educativa Técnico Industrial sede Mercedes Pardo de Simmonds para la ejecución de sus actividades en el proceso de gestión académica.

Identificar y valorar los activos de información disponible en la Institución Educativa Técnico Industrial sede Mercedes Pardo de Simmonds.

Identificar los posibles riesgos de los activos de información, sus vulnerabilidades y amenazas, así como su probabilidad de ocurrencia y el impacto de los mismos.

Realizar un análisis al aplicativo web de calificaciones orientado a identificar las vulnerabilidades que ponen en riesgo la seguridad de la información de la Institución Educativa Técnico Industrial sede Mercedes Pardo de Simmonds.

Presentar el diagnóstico del estado actual de la seguridad de la información de la Institución Educativa Técnico Industrial sede Mercedes Pardo de Simmonds con sus respectivas recomendaciones de mejora y de implementación basado en la norma ISO 27001:2013

Metodología

El presente proyecto se basó en el análisis cualitativo de la organización mediante el diagnóstico de la seguridad de la información aplicado al proceso gestión académica, el análisis se basó en la norma ISO 27001: 2013 para la identificación de las amenazas, vulnerabilidades y riesgos, la probabilidad de ocurrencia y el impacto en caso de materialización.

Se realizó un reconocimiento del funcionamiento general, que permitió tener una visión macro de los procesos realizados y poder enfocarse posteriormente en el conocimiento específico y detallado del proceso gestión académica que fue el seleccionado para el desarrollo del presente proyecto; una vez reconocido los procedimientos realizados en este proceso se hizo un análisis de la información recolectada que permitió hacer una evaluación de riesgos y poder realizar un diagnóstico a la seguridad de la información basada en la norma ISO 27001:2013, con el fin de disminuir el impacto y probabilidad de ocurrencia de vulnerabilidades, amenazas y riesgos a la que está expuesta la institución Educativa Sede Mercedes Pardo de Simmonds de la ciudad de Popayán y de esta manera poder presentar los controles adecuados y su debidas recomendaciones al proceso seleccionado.

Resultados

En el análisis realizado al proceso gestión académica se identificaron 20 no conformidades, 9 de tipo mayor y 11 no conformidades de tipo menor como se describen a continuación:

no conformidades de tipo mayor

- Políticas de seguridad de la información y revisión de estas, Roles y responsabilidades para la seguridad de la información, clasificación de la información, Etiquetado de la información, Política sobre el uso de controles criptográficos, Equipo de usuario desatendido, Copias de respaldo de la información, Políticas y procedimientos para el intercambio de información, Gestión de los incidentes de la seguridad de la información

No conformidades de tipo menor

- Política de control de acceso, Acceso a redes y a servicios de red, Sistema de gestión de contraseñas, Servicios de suministro, Política de escritorio despejado y de pantalla despejada, El control de acceso contra código malicioso, Instalación de software en sistemas operacionales, Controles de auditorías de sistemas de información, Política de desarrollo seguro, Planificación de la continuidad de la seguridad de la información, Privacidad y protección de información de datos personales

Conclusiones

De acuerdo a los resultados arrojados en el desarrollo del proyecto se puede decir que la falta de conocimiento sobre la importancia de la seguridad de la información, como uno de los mayores activos de la organización, conlleva a un conjunto de malas prácticas dentro de los procedimientos realizados, de omisión de responsabilidades en los diferentes cargos por desconocimiento o por la falta de implementación de políticas de seguridad que permitan proteger adecuadamente la información del proceso gestión académica.